GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

SIXTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2021

© Law Business Research 2021

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2021
For further information please contact insight@globalinvestigationsreview.com

© Law Business Research 2021

The Practitioner's Guide to Global Investigations

Sixth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Celeste Koeleveld

© Law Business Research 2021

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK
© 2020 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
natalie.hacker@lbresearch.com
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-272-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

ABB Ltd

Addleshaw Goddard LLP

Anagnostopoulos

Association of Corporate Investigators

Baker McKenzie LLP

BCL Solicitors LLP

BDO USA, LLP

Blank Rome LLP

Booking.com

Brown Rudnick LLP

Cadwalader, Wickersham & Taft LLP

Claro y Cia

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Corker Binning

Cravath, Swaine & Moore LLP

Debevoise & Plimpton LLP

DLA Piper LLP

Fornari e Associati

Fountain Court Chambers

Fox Williams LLP

Freshfields Bruckhaus Deringer LLP

Gleiss Lutz

Goodwin

Herbert Smith Freehills

© Law Business Research 2021

Homburger

Jenner & Block

Jones Day

Kingsley Napley LLP

Latham & Watkins

Linklaters LLP

McGuireWoods

Marval O'Farrell Mairal

Matheson

Mayer Brown

Meredith Connell

Mishcon de Reya LLP

Navacelle

Noerr

Nokia Corporation

Norton Rose Fulbright LLP

Outer Temple Chambers

Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pinsent Masons LLP

Rebaza, Alcázar & De Las Casas

Reed Smith LLP

Ropes & Gray LLP

Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Slaughter and May

Sullivan & Cromwell LLP

Trench Rossi Watanabe

Uría Menéndez Abogados, SLP

Walden Macht & Haran LLP

Willkie Farr & Gallagher LLP

© Law Business Research 2021

Publisher's Note

The Practitioner's Guide to Global Investigations is published by Global Investigations Review (www.globalinvestigationsreview.com) – a news and analysis service for lawyers and related professionals who specialise in cross-border white-collar crime investigations.

The Guide was suggested by the editors to fill a gap in the literature – namely, how does one conduct (or conduct oneself) in such an investigation, and what should one have in mind at various times?

It is published annually as a two-volume work and is also available online and in PDF format.

The volumes

This Guide is in two volumes. Volume I takes the reader through the issues and risks faced at every stage in the life cycle of a serious corporate investigation, from the discovery of a potential problem through its exploration (either by the company itself, a law firm or government officials) all the way to final resolution – be that in a regulatory proceeding, a criminal hearing, civil litigation, an employment tribunal, a trial in the court of public opinion, or, just occasionally, inside the company's own four walls. As such it uses the position in the two most active jurisdictions for investigations of corporate misfeasance – the United States and the United Kingdom – to illustrate the practices and thought processes of cutting-edge practitioners, on the basis that others can learn much from their approach, and there is a read-across to the position elsewhere.

Volume II takes a granular look at law, regulation, enforcement and best practice in the jurisdictions around the world with the most active corporate investigations spaces, highlighting, among other things, where they vary from the norm.

Online

The Guide is available at www.globalinvestigationsreview.com. Containing the most up-to-date versions of the chapters in Volume I, the website also allows visitors to quickly compare answers to questions in Volume II across all the jurisdictions covered.

The publisher would like to thank the editors for their exceptional energy, vision and intellectual rigour in devising and maintaining this work. Together we welcome any comments or suggestions from readers on how to improve it. Please write to us at: insight@globalinvestigationsreview.com.

© Law Business Research 2021

Foreword

Mary Jo White

Partner and Senior Chair, Debevoise & Plimpton LLP; Former Chair, US Securities and Exchange Commission; Former US Attorney for the Southern District of New York

The sixth edition of GIR's *The Practitioner's Guide to Global Investigations* is emblematic of the important work GIR has now done for many years, making sure that the lawyers and others who practise in the field have the resources and information they need to stay current in a transforming world. Compared with white-collar practice when I began my career, the landscape today can seem dizzying in its ever-expanding complexity. The amount of data now available, and the variety of means of communication, are boundless. Pitfalls are everywhere, from new and sometimes conflicting rules on data privacy to varied and changing standards for the attorney–client privilege across the world, among many others. The talented editors and very knowledgeable authors of this treatise, many of whom I have had the pleasure of working with first-hand throughout the course of my careers in government and now again in private practice, have done us all a great service in producing this valuable and practical resource.

The Guide tracks the life cycle of a serious issue, from its discovery through investigation and resolution, and the many steps, considerations and decisions along the way – and, at each critical point, includes chapters from the perspective of experienced practitioners from both the United States and the United Kingdom, and at times other jurisdictions. The chapters provide invaluable advice for the most experienced practitioners and a useful orientation for lawyers who may be new to the subject matter and are full of practical considerations based on a wealth of experience among the authors, who represent many of the leading law firms around the world, including my own. Unlike many other treatises, the Guide also offers separate – and essential – perspectives from leading in-house lawyers and from outside consultants who are critical parts of the investigative team, including forensic accountants and public relations experts.

The comparative approach of this book is unique, and it is uniquely helpful. Having the US and UK chapters side by side in Volume I can deepen understanding for even veteran practitioners by highlighting the different (and sometimes significantly divergent) approaches to key issues, just as learning a foreign language deepens our understanding of a native tongue. These comparisons, as well as the primers for other regions around the world in Volume II, are an essential guidebook for fostering clear communications across international legal and cultural boundaries. Many a misunderstanding could be avoided

© Law Business Research 2021

by starting with this book when a new cross-border issue arises, and appreciating that we bring to each legal problem internalised frameworks that have become so familiar as to be invisible to us. The comparative approach of this treatise shines a light on those differences, and can prevent many missteps.

There are also very helpful situational comparisons, including chapters on interviewing witnesses when representing a corporation but also from the perspective of representing the individual. A lawyer on either side will benefit from reading the chapter on the other perspective.

The specific chapter topics in the Guide are a checklist for the many complexities of modern cross-border investigations, including considerations of self-reporting and co-operation, extraterritorial jurisdiction, remediation and dealing with monitorships. Significant attention is given to electronic data collection and strategies for using it to best advantage, and appropriately so. In almost any modern investigation, the amount of electronic data available to investigators will far exceed the resources that reasonably can be applied to reviewing it. Developing a well targeted but adaptive strategy for turning these mountains of data into actionable investigative information is absolutely critical, both to understanding the issue in a timely fashion and in delivering value to clients. The proliferation of stringent but diverse data privacy laws only adds to the complexity in this process, and the Guide is right to emphasise that understanding these issues early on is essential to the success of any cross-border investigation.

The Guide's chapters on negotiating global settlements are spot on. Despite professed global and domestic agreement against 'piling on', it remains a rarity to have only a single enforcement authority or regulator involved in a significant case. And although it is now accepted wisdom – and in my experience, the reality – that authorities across the globe are coordinating more than ever, this coordination does not mean the end of competition among them. As we frequently see in the United States, competition – even among authorities and regulators in the same jurisdiction – is still the frustrating norm. All of this amplifies both the risks that significant issues can bring, and the challenge for counsel to understand the competing perspectives that are at play.

The jurisdictional surveys in the second volume are also a tremendous resource when we confront a problem in an unfamiliar locale. These are necessarily high-level, but they can help identify the important questions that need to be asked at an early stage. As any good investigator can attest, knowing the right questions to ask is often more than half the battle.

This sixth edition arrives just as many of us are looking forward to returning to the office and to travel, meeting more people and investigations face to face. As predicted in the previous volume, the strain and disruption of the pandemic has only increased the number of serious issues requiring inquiry across the globe. The Guide will be a tremendous benefit to the practitioners who take them on – particularly for those who consult it early and often.

New York
November 2021
mjwhite@debevoise.com

© Law Business Research 2021

Preface

The history of the global investigation

For over a decade, the number and profile of multi-agency, multi-jurisdictional regulatory and criminal investigations have risen exponentially. Naturally, this global phenomenon exposes companies – and their employees – to greater risk of hostile encounters with foreign law enforcers and regulators than ever. This is partly owing to the continued globalisation of commerce, the increasing enthusiasm of some prosecutors to use expansive theories of corporate criminal liability to exact exorbitant penalties as a deterrent and public pressure to hold individuals accountable for the misconduct. The globalisation of corporate law enforcement, of course, has also spawned greater coordination between law enforcement agencies, domestically and across borders. As a result, the pace and complexity of cross-border corporate investigations has markedly increased and created an environment in which the potential consequences, direct and collateral, for individuals and businesses, are unprecedented.

The Guide

To aid practitioners faced with the challenges of steering a course through a cross-border investigation, this Guide brings together the perspectives of leading experts from across the globe.

The chapters in Volume I cover, in depth, the broad spectrum of law, practice and procedure applicable to investigations in the United Kingdom and United States. The Volume tracks the development of a serious allegation (originating from an internal or external source) through all its stages, flagging the key risks and challenges at each step; it provides expert insight into the fact-gathering phase, document preservation and collection, witness interviews, and the complexities of cross-border privilege issues; it discusses strategies to successfully resolve international probes and manage corporate reputation throughout; and it covers the major regulatory and compliance issues that investigations invariably raise.

In Volume II, local experts from major jurisdictions across the globe respond to a common and comprehensive set of questions designed to identify the local nuances of law and practice that practitioners may encounter in responding to a cross-border investigation.

In the first edition, we signalled our intention to update and expand both parts of the book as the rules evolve and prosecutors' appetites change. The Guide continues to grow in substance and geographical scope. By its third edition, it had outgrown the original

© Law Business Research 2021

single-book format. The two parts of the Guide now have separate covers, but the hard copy should still be viewed – and used – as a single reference work. All chapters are, of course, made available online and in other digital formats.

Volume I, which is bracketed by comprehensive tables of law and a thematic index, has been wholly revised to reflect developments over the past year. These range from US prosecutors reprising their previously uncompromising approach to pursuing *all* individuals involved in corporate misconduct and promising a surge in enforcement activity to UK authorities securing a raft of deferred prosecution agreements, some of which remain under reporting restrictions at the time of going to press. For this edition, we have commissioned a new chapter on emerging standards for companies' ESG – environmental, social and governance – practices. This issue has rocketed to the top of corporate agendas, and raised the eyebrows of legislators and regulators, far and wide. The Editors feel that this is an area to watch closely and that corporate ESG investigations will proliferate in the coming years.

The revised, expanded questionnaire for Volume II includes a new section on ESG issues so readers can gauge the developments in each jurisdiction profiled. Volume II carries regional overviews giving insight into cultural issues and regional coordination by authorities. The second volume now covers 21 jurisdictions in the Americas, the Asia-Pacific region and Europe. As corporate investigations and enforcer co-operation cross more borders, we anticipate Volume II will become increasingly valuable to our readers: external and in-house counsel; compliance and accounting professionals; and prosecutors and regulators operating in this complex environment.

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Celeste Koeleveld
December 2021
London, New York and Washington, DC

© Law Business Research 2021

Contents

Foreword v
Preface vii
Contents ix
Table of Cases xxv
Table of Legislation liii

VOLUME I
GLOBAL INVESTIGATIONS IN THE UNITED KINGDOM AND THE UNITED STATES

1 Introduction to Volume I 1
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Celeste Koeleveld

1.1 Bases of corporate criminal liability 2
1.2 Double jeopardy 10
1.3 The stages of an investigation 23

2 The Evolution of Risk Management in Global Investigations 31
William H Devaney, Joanna Ludlam, Mary Jordan and Aleesha Fowler

2.1 Introduction 31
2.2 Sources and triggers of corporate investigations 31
2.3 The challenges of conducting remote investigations 43
2.4 ESG issues 44
2.5 Corporate legal and compliance functions: who should investigate? 46

© Law Business Research 2021

3 Self-Reporting to the Authorities and Other Disclosure Obligations: The UK Perspective 47
Judith Seddon, Amanda Raad, Sarah Lambert-Porter and Matthew Burn

3.1 Introduction 47
3.2 Culture and whistleblowing 49
3.3 The evolution of the link between self-reporting and a DPA 52
3.4 Obligatory self-reporting 52
3.5 Voluntary self-reporting to the SFO 60
3.6 Advantages of self-reporting 61
3.7 Risks in self-reporting 70
3.8 Practical considerations, step by step 76

4 Self-Reporting to the Authorities and Other Disclosure Obligations: The US Perspective 80
Amanda Raad, Sean Seelinger, Jaime Orloff Feeney and Zaneta Wykowska

4.1 Introduction 80
4.2 Mandatory self-reporting to authorities 81
4.3 Voluntary self-reporting to authorities 83
4.4 Risks in voluntarily self-reporting 92
4.5 Risks in choosing not to self-report 93

5 Beginning an Internal Investigation: The UK Perspective 96
Jonathan Cotton, Holly Ware and Ella Williams

5.1 Introduction 96
5.2 Whether to notify any relevant authorities 96
5.3 Whether and when to launch an internal investigation 98
5.4 Oversight and management of the investigation 100
5.5 Scoping the investigation 101
5.6 Document preservation, collection and review 102

© Law Business Research 2021

6 Beginning an Internal Investigation: The US Perspective..... 107
Bruce E Yannett and David Sarratt

6.1 Introduction 107
6.2 Assessing if an internal investigation is necessary 107
6.3 Identifying the client 111
6.4 Control of the investigation: in-house or external counsel 111
6.5 Determining the scope of the investigation 112
6.6 Document preservation, collection and review 115
6.7 Documents located abroad 118

7 Witness Interviews in Internal Investigations: The UK Perspective..... 121
Caroline Day and Louise Hodges

7.1 Introduction 121
7.2 Types of interviews 122
7.3 Deciding whether authorities should be consulted 123
7.4 Providing details of the interviews to the authorities 125
7.5 Identifying witnesses and the order of interviews 128
7.6 When to interview 130
7.7 Planning for an interview 132
7.8 Conducting the interview: formalities and separate counsel 133
7.9 Conducting the interview: whether to caution the witness 135
7.10 Conducting the interview: record-keeping 136
7.11 Legal privilege in witness interviews 137
7.12 Conducting the interview: employee amnesty and self-incrimination 142
7.13 Considerations when interviewing former employees 143
7.14 Considerations when interviewing employees abroad 144
7.15 Key points 145

© Law Business Research 2021

8 Witness Interviews in Internal Investigations: The US Perspective 147
Anne M Tompkins, Jodi Avergun and J Robert Duncan

8.1 Introduction 147
8.2 Preparation for the interview 147
8.3 Upjohn protections 149
8.4 Protecting work-product and attorney–client privilege 149
8.5 Note-taking and privilege 150
8.6 Interactions with witnesses 152
8.7 Document review and selection 153
8.8 Remote interviews: costs and covid-security 153
8.9 Reporting the results of interviews 154
8.10 Conclusion 155

9 Co-operating with the Authorities: The UK Perspective 156
Matthew Bruce, Ali Kirby-Harris, Ben Morgan and Ali Sallaway

9.1 Introduction 156
9.2 The status of the corporate and other initial considerations 157
9.3 What does co-operation mean? 158
9.4 Co-operation can lead to reduced penalties 167
9.5 Compliance 170
9.6 New management 170
9.7 Companies tend to co-operate for a number of reasons 171
9.8 Multi-agency and cross-border investigations 172
9.9 Strategies for dealing with multiple authorities 173
9.10 Conclusion 173

10 Co-operating with the Authorities: The US Perspective 175
John D Buretta, Megan Y Lew and Jingxi Zhai

10.1 What is co-operation? 175
10.2 Key benefits and drawbacks to co-operation 188
10.3 Special challenges with multi-agency and cross-border investigations 196

© Law Business Research 2021

11 Production of Information to the Authorities 202
Pamela Reddy, Kevin Harnisch, Katie Stephen, Andrew Reeves and Ilana Sinkin

11.1 Introduction 202
11.2 UK regulators 204
11.3 US regulators 209
11.4 Privilege 211
11.5 Cross-border investigations and considerations 213

12 Production of Information to the Authorities: The In-house Perspective 218
Femi Thomas, Tapan Debnath and Daniel Igra

12.1 Introduction 218
12.2 Initial considerations 218
12.3 Data collection and review 219
12.4 Principal concerns for corporates contemplating production 220
12.5 Obtaining material from employees 223
12.6 Material held overseas 225
12.7 Concluding remarks 226

13 Employee Rights: The UK Perspective 229
James Carlton, Sona Ganatra and David Murphy

13.1 Contractual and statutory employee rights 229
13.2 Representation 233
13.3 Indemnification and insurance coverage 235
13.4 Privilege concerns for employees and other individuals 238

14 Employee Rights: The US Perspective 240
Milton L Williams, Avni P Patel and Jacob Gardener

14.1 Introduction 240
14.2 The right to be free from retaliation 241
14.3 The right to representation 243
14.4 The right to privacy 244
14.5 Covid-19 246
14.6 Indemnification 248
14.7 Situations where indemnification may cease 251
14.8 Privilege concerns for employees 251

© Law Business Research 2021

15 Representing Individuals in Interviews: The UK Perspective 253
Jessica Parker and Andrew Smith

15.1 Introduction 253
15.2 Interviews in corporate internal investigations 253
15.3 Interviews of witnesses in law enforcement investigations 257
15.4 Interviews of suspects in law enforcement investigations 260
15.5 Representing individuals during the pandemic 262

16 Representing Individuals in Interviews: The US Perspective 264
John M Hillebrecht, Lisa Tenorio-Kutzkey and Eric Christofferson

16.1 Introduction 264
16.2 Kind and scope of representation 264
16.3 Whether to be interviewed 267
16.4 Preparation for interview 268
16.5 Procedures for government interview 271
16.6 Conclusion 274

17 Individuals in Cross-Border Investigations or Proceedings: The UK Perspective 275
Richard Sallybanks, Anoushka Warlow and Alex Swan

17.1 Introduction 275
17.2 Cross-border co-operation 275
17.3 Practical issues 277
17.4 Extradition 283
17.5 Settlement considerations 289
17.6 Reputational considerations 290

© Law Business Research 2021

18 Individuals in Cross-Border Investigations or Proceedings: The US Perspective 291
Amanda Raad, Michael McGovern, Meghan Gilligan Palermo, Zaneta Wykowska, Abraham Lee and Chloe Gordils

18.1 Introduction 291
18.2 Preliminary considerations 293
18.3 Extradition 295
18.4 Strategic considerations 306
18.5 Evidentiary issues 314
18.6 Asset freezing, seizure and forfeiture 317
18.7 Collateral consequences 319
18.8 The human element: client-centred lawyering 319

19 Whistleblowers: The UK Perspective 321
Alison Wilson, Sinead Casey, Elly Proudlock and Nick Marshall

19.1 Introduction 321
19.2 The legal framework 321
19.3 The corporate perspective: representing the firm 328
19.4 The individual perspective: representing the individual 334

20 Whistleblowers: The US Perspective 337
Daniel Silver and Benjamin A Berringer

20.1 Overview of US whistleblower statutes 337
20.2 The corporate perspective: preparation and response 344
20.3 The whistleblower's perspective: representing whistleblowers 349
20.4 Filing a qui tam action under the False Claims Act 355

21 Whistleblowers: The In-house Perspective 360
Steve Young

21.1 Initial considerations 360
21.2 Identifying legitimate whistleblower claims 362
21.3 Employee approaches to whistleblowers 362
21.4 Distinctive aspects of investigations involving whistleblowers 363
21.5 The covid-19 pandemic and whistleblowing 364
21.6 The European Union Whistleblower Directive 365
21.7 International Standards Organisation whistleblowing management systems 366

© Law Business Research 2021

22 Forensic Accounting Skills in Investigations 368
Glenn Pomerantz and Daniel Burget

22.1 Introduction 368
22.2 Regulator expectations 369
22.3 Preservation, mitigation and stabilisation 370
22.4 e-Discovery and litigation holds 370
22.5 Violation of internal controls 371
22.6 Forensic data science and analytics 372
22.7 Analysis of financial data 376
22.8 Analysis of non-financial records 377
22.9 Use of external data in an investigation 379
22.10 Review of supporting documents and records 382
22.11 Tracing assets and other methods of recovery 383
22.12 Cryptocurrencies 384
22.13 Conclusion 385

23 Negotiating Global Settlements: The UK Perspective 386
Nicholas Purnell QC, Brian Spiro and Jessica Chappatte

23.1 Introduction 386
23.2 Initial considerations 392
23.3 Legal considerations 411
23.4 Practical issues arising from the negotiation of UK DPAs 413
23.5 Resolving parallel investigations 419

24 Negotiating Global Settlements: The US Perspective 421
Nicolas Bourtin

24.1 Introduction 421
24.2 Strategic considerations 421
24.3 Legal considerations 427
24.4 Forms of resolution 431
24.5 Key settlement terms 437
24.6 Resolving parallel investigations 445

© Law Business Research 2021

25 Fines, Disgorgement, Injunctions, Debarment: The UK Perspective 449

Tom Epps, Marie Kavanagh, Andrew Love, Julia Maskell and Benjamin Sharrock

25.1 Criminal financial penalties 449
25.2 Compensation 450
25.3 Confiscation 450
25.4 Fine 452
25.5 Guilty plea 453
25.6 Costs 454
25.7 Director disqualifications 455
25.8 Civil recovery orders 455
25.9 Criminal restraint orders 457
25.10 Serious crime prevention orders 457
25.11 Regulatory financial penalties and other remedies 458
25.12 Withdrawing a firm's authorisation 460
25.13 Approved persons 461
25.14 Restitution orders 461
25.15 Debarment 462
25.16 Outcomes under a DPA 463

26 Fines, Disgorgement, Injunctions, Debarment: The US Perspective 465

Anthony S Barkow, Charles D Riely, Amanda L Azarian and Grace C Signorelli-Cassady

26.1 Introduction 465
26.2 Standard criminal fines and penalties available under federal law 467
26.3 Civil penalties 470
26.4 Disgorgement and prejudgment interest 472
26.5 Injunctions 474
26.6 Other consequences 475
26.7 Remedies under specific statutes 476
26.8 Conclusion 481

© Law Business Research 2021

27 Global Settlements: The In-house Perspective 482
Claire McLeod

27.1 Introduction 482
27.2 Senior management 482
27.3 Shareholders 485
27.4 Employees 485
27.5 Customers 486
27.6 Regulators and enforcement agencies 487
27.7 Conclusion 489

28 Extraterritoriality: The UK Perspective 490
Anupreet Amole, Aisling O'Sullivan and Francesca Cassidy-Taylor

28.1 Overview 490
28.2 The Bribery Act 2010 491
28.3 The Proceeds of Crime Act 2002 494
28.4 Tax evasion and the Criminal Finances Act 2017 498
28.5 Financial sanctions 499
28.6 Conspiracy 502
28.7 Mutual legal assistance, cross-border production and the extraterritorial authority of UK enforcement agencies 504

29 Extraterritoriality: The US Perspective 507
James P Loonam and Ryan J Andreoli

29.1 Extraterritorial reach of US laws 507
29.2 Securities laws 508
29.3 Criminal versus civil cases 514
29.4 RICO 517
29.5 Wire fraud 518
29.6 Commodity Exchange Act 520
29.7 Antitrust 523
29.8 Foreign Corrupt Practices Act 527
29.9 Sanctions 530
29.10 Money laundering 532
29.11 Power to obtain evidence located overseas 534
29.12 Conclusion 535

© Law Business Research 2021

30 Individual Penalties and Third-Party Rights: The UK Perspective 536
Elizabeth Robertson, Vanessa McGoldrick and Jason Williamson

30.1 Individuals: criminal liability 536
30.2 Individuals: regulatory liability 546
30.3 Other issues: UK third-party rights 547

31 Individual Penalties and Third-Party Rights: The US Perspective 549
Todd Blanche and Cheryl Risell

31.1 Prosecutorial discretion 549
31.2 Sentencing 556

32 Extradition 562
Ben Brandon and Aaron Watkins

32.1 Introduction 562
32.2 Bases for extradition 563
32.3 Core concepts 564
32.4 Trends in extradition 567
32.5 Contemporary issues in extradition 570

33 Monitorships 576
Robin Barclay QC, Nico Leslie, Christopher J Morvillo, Celeste Koeleveld and Meredith George

33.1 Introduction 576
33.2 Evolution of the modern monitor 578
33.3 Circumstances requiring a monitor 585
33.4 Selecting a monitor 590
33.5 The role of the monitor 595
33.6 Costs and other considerations 605
33.7 Conclusion 606

© Law Business Research 2021

34 Parallel Civil Litigation: The UK Perspective 607
Nichola Peters and Michelle de Kluyver

34.1 Introduction 607
34.2 Stay of proceedings 607
34.3 Multi-party litigation 609
34.4 Derivative claims and unfair prejudice petitions 614
34.5 Securities litigation 616
34.6 Other private litigation 618
34.7 Evidentiary issues 627
34.8 Practical considerations 631
34.9 Concurrent settlements 632
34.10 Concluding remarks 633

35 Parallel Civil Litigation: The US Perspective..... 634
David B Hennes, Lisa H Bebchick, Alexander B Simkin, Patrick T Roath and Jeel Oza

35.1 Introduction 634
35.2 Stay of proceedings 635
35.3 Potential types of parallel civil litigation 639
35.4 Evidentiary issues 648
35.5 Additional practical considerations 650
35.6 Conclusion 655

36 Privilege: The UK Perspective..... 656
Tamara Oppenheimer QC, Rebecca Loveridge and Samuel Rabinowitz

36.1 Introduction 656
36.2 Legal professional privilege: general principles 657
36.3 Legal advice privilege 662
36.4 Litigation privilege 675
36.5 Common interest privilege 684
36.6 Without prejudice privilege 688
36.7 Exceptions to privilege 692
36.8 Loss of privilege and waiver 699
36.9 Maintaining privilege: practical issues 708

© Law Business Research 2021

37 Privilege: The US Perspective 715
Richard M Strassberg and Meghan K Spillane

37.1 Privilege in law enforcement investigations 715
37.2 Identifying the client 723
37.3 Maintaining privilege 725
37.4 Waiving privilege 730
37.5 Selective waiver 736
37.6 Taint teams 739
37.7 Disclosure to third parties 741
37.8 Expert witnesses 747

38 Publicity: The UK Perspective 749
Kevin Roberts, Duncan Grieve and Charlotte Glaser

38.1 Introduction 749
38.2 Before the commencement of an investigation or prosecution 749
38.3 Following the commencement of an investigation or prosecution 751
38.4 Following the conclusion of an investigation or prosecution 752
38.5 Legislation governing the publication of information 753
38.6 The changing landscape: remote hearings and open justice 759

39 Publicity: The US Perspective 760
Jodi Avergun

39.1 Restrictions in a criminal investigation or trial 760
39.2 Social media and the press 769
39.3 Risks and rewards of publicity 772

40 Data Protection in Investigations 776
Stuart Alford QC, Serrin A Turner, Gail E Crawford, Hayley Pizzey, Mair Williams and Matthew Valenti

40.1 Introduction 776
40.2 Internal investigations: UK perspective 778
40.3 Internal investigations: US perspective 786
40.4 Investigations by authorities: UK perspective 788
40.5 Investigations by authorities: US perspective 790
40.6 Whistleblowers 792
40.7 Collecting, storing and accessing data: practical considerations 793

© Law Business Research 2021

41 Cybersecurity 794
Francesca Titus, Andrew Thornton-Dibb, Rodger Heaton, Mehboob Dossa and William Boddy

41.1 Introduction 794
41.2 Legal framework 800
41.3 Proactive cybersecurity 806
41.4 Conducting an effective investigation into a cyber breach 807
41.5 Enforcement 808

42 Directors' Duties: The UK Perspective 811
Nichola Peters, Michelle de Kluyver and Jaya Gupta

42.1 Introduction 811
42.2 Sources of directors' duties and responsibilities under UK law 812
42.3 Expectations, not obligations 830
42.4 Conclusion 830

43 Directors' Duties: The US Perspective 831
Daniel L Stein, Jason Linder, Glenn K Vanzura and Bradley A Cohen

43.1 Introduction 831
43.2 Directors' fiduciary duties 832
43.3 Liability for breach of fiduciary duties 835
43.4 Regulatory enforcement actions 837
43.5 SEC Whistleblower Program 839
43.6 Duty of oversight in investigations 840
43.7 Strategic considerations for directors 841

44 Sanctions: The UK Perspective 843
Rita Mitchell, Simon Osborn-King and Yannis Yuen

44.1 Introduction 843
44.2 Overview of the UK sanctions regime 844
44.3 Offences and penalties 848
44.4 Sanctions investigations 849
44.5 Best practices in investigations 851
44.6 Trends and key issues 855

© Law Business Research 2021

45 Sanctions: The US Perspective 859
David Mortlock, Britt Mosman, Nikki Cronin and Ahmad El-Gamal

45.1 Overview of the US sanctions regime 859
45.2 Offences and penalties 866
45.3 Commencement of sanctions investigations 867
45.4 Enforcement 867
45.5 Trends and key issues 872

46 Compliance 875
Alison Pople QC, Johanna Walsh and Mellissa Curzon-Berners

46.1 Introduction 875
46.2 UK criminal liability for corporate compliance failures 876
46.3 UK regulatory liability for corporate compliance failures 879
46.4 Compliance guidance 880
46.5 The interplay between culture and effective compliance 888
46.6 The impact of compliance on prosecutorial decision-making 890
46.7 Key compliance considerations from previous resolutions 892
46.8 Conclusion 895

47 Environmental, Social and Governance Investigations 897
Emily Goddard, Anna Kirkpatrick and Ellen Lake

47.1 Introduction 897
47.2 ESG issues and investigation triggers 897
47.3 The legal and regulatory frameworks 900
47.4 Particularities of ESG-related investigations 904

Appendix 1: About the Authors of Volume I 911
Appendix 2: Contributors' Contact Details 963
Index to Volume I 971

© Law Business Research 2021

Table of Cases

United Kingdom

3M v. Rennicks, Unreported, 1 October 1990 21–1
A v. B and Financial Reporting Council [2020] EWHC 1491 ..... 36.2.5
Addlesee v. Dentons Europe LLP [2019] EWCA Civ 1600, [2020] Ch 243 ..... 36.2.2, 36.7.1
Aegis Blaze, The [1986] 1 Lloyd's Rep 203 ..... 36.4.2
Ainsworth v. Wilding [1900] 2 Ch 315 ..... 36.3.1
AJ & DJ, Re, Unreported, 9 December 1992, CA 25.9
Akcine Bendrove Bankas Snoras (In Bankruptcy) v. Antonov [2013] EWHC 131 (Comm) 34.2.1
AL v. SFO. *See* R (on the application of AL) v. Serious Fraud Office
Al-Fayed v. Commissioner of Police of the Metropolis [2002] EWCA Civ 780 ..... 36.8.3
Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs (No. 2) [1972] 2 QB 102, 129 CA 36.3.2.1
Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs (No. 2) [1974] AC 405 HL 36.3.2.1
Alphacell Ltd v. Woodward [1972] AC 824 ..... 9.3
Anderson v. Bank of British Columbia (1876) 2 Ch D 644 ..... 36.2.3
Arnott, Ex p. Chief Official Receiver, Re (1888) 60 LT 109 ..... 36.2.1
Ashburton v. Pape [1913] 2 Ch 469, CA 36.2.2
Assange v. Swedish Prosecution Auth [2011] EWHC 2849 ..... 18.3
Astex v. Astrazeneca [2016] EWHC 2759 (Ch) 36.3.2.2
Attorney General v. Guardian Newspapers Ltd (No. 2) [1990] 1 AC 109 ..... 36.8
Attorney General's Reference (No. 2 of 1999) [2000] 2 Cr App R 207 ..... 1.1.1, 9.3
B v. Auckland District Law Society [2003] 2 AC 736 ..... 36.2.2, 36.7.2, 36.8.1
Babula v. Waltham Forest College (2007) EWCA Civ 174 ..... 19.2.1.3
Bachnak v. Emerging Markets Partnership Europe (2006) UKEAT/0288/05/RN 19.2.1.3
Balabel v. Air India [1988] 1 Ch 317 ..... 7.11, 36.3.1, 36.3.2.2, 36.3.3
Bank of Nova Scotia v. Hellenic Mutual War Risks Association (Bermuda) Ltd (The Good Luck) [1992] 2 Lloyd's Rep 540 ..... 36.3.1, 36.5
Banque Keyser Ullman SA v. Skandia (UK) Insurance Co Ltd [1986] 1 Lloyd's Rep 336 ..... 36.7.1
Barclays Bank v. Eustice [1995] 1 WLR 1238 ..... 36.7.1
Barings Plc (No. 5), Re, Secretary of State for Trade and Industry v. Baker [1999] 1 BCLC 433 ..... 42.2.1.4
Barnetson v. Framlingham Group [2007] 1 WLR 2443 (CA) 36.6
BBGP Managing General Partner Ltd v. Babcock and Brown [2011] Ch 296 ..... 36.7.1
Belhaj v. DPP [2018] EWHC 513 (Admin) 36.8.1
Berezovsky v. Hine [2011] EWCA Civ 1089 ..... 36.8.1

© Law Business Research 2021

Berkeley Square Holdings v. Lancer Property Asset Management Ltd [2020] EWHC 1015 (Ch) 36.6
Bilta (UK) Ltd (In Liquidation) v. Royal Bank of Scotland and Mercuria Energy Europe Trading Ltd [2017] EWHC 3535 (Ch) 7.11, 12.4, 23.2.2.1, 28.7, 34.7.3, 36.4.3
Bolkiah v. KPMG [1999] 2 AC 222, HL 36.2.5
Bolton Engineering Co v. Graham [1957] 1 QB 159 ..... 7.5, 23.1
Bourns Inc v. Raychem Corp [1999] 3 All ER 154, CA 36.2.1
Bowman v. Fels [2005] 1 WLR 3083, CA 36.7.2
Bradcrown Ltd, Re [2002] BCC 428; [2001] 1 BCLC 547 ..... 42.2.1.4
Bradford & Bingley plc v. Rashid [2006] 1 WLR 2066 ..... 36.6
Bravo and Others v. Amerisur Resources Plc [2020] EWHC 203 (QB) 34.3.3
British Home Stores Ltd v. Burchell [1978] UKEAT 108_78_2007 ..... 7.12
Bunbury v. Bunbury (1839) 2 Beav 173 ..... 36.3.2.1
Bursill v. Tanner (1885) 16 QBD 1 ..... 36.2.1
Butler v. Board of Trade [1971] 1 Ch 680 ..... 36.7.1
Buttes Gas and Oil Co v. Hammer (No. 3) [1982] AC 888, HL 36.4.1, 36.5
Calcraft v. Guest [1898] 1 QB 759, CA 36.2.2
Cape Intermediate Holdings Ltd v. Dring [2019] UKSC 38, [2019] 3 WLR 429 ..... 38.5.1.1
Cathcart Ex p. Campbell, Re (1869–70) LR 5 Ch App 703 ..... 36.2.1
Cheng v. Governor of Pentonville Prison [1973] AC 931 ..... 32.3.3
Chesterton Global and Verman v. Nurmohamed (2017) EWCA Civ 979 ..... 19.2.1.3
China Export & Credit Insurance Corporation v. Emerald Energy Resources Limited [2018] EWHC 1503 (Comm) 34.2.1
Clyde & Co LLP v. Bates van Winkelhof (2014) UKSC 32 ..... 19.2.1
Coleman Taymar Ltd v. Oakes [2001] 2 BCLC 749 ..... 42.2.1.4
Commercial Union Assurance Co Plc v. Mander [1996] 2 Lloyd's Rep 640 ..... 36.5
Continental Assurance Co of London Plc (In Liquidation). *See* Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig
Crawford v. Suffolk Mental Health Partnership NHS Trust [2012] IRLR 402 ..... 13.1.2
Crescent Farm (Sidcup) Sports Ltd v. Sterling Offices Ltd [1972] Ch 553 ..... 36.7.1
Curless v. Shell Ltd [2019] EWCA Civ 1710 ..... 36.7.1
Dadourian Group International v. Simms [2008] EWHC 1784 (Ch) 36.3.2.1
Dechert v. ENRC. *See* Eurasian Natural Resources Corp Ltd v. Dechert LLP
Depp II v. News Group Newspaper Ltd [2020] EWHC 2911 (QB) 38.5.1.2
Derby & Co Ltd v. Weldon (No. 7) [1990] 1 WLR 1156 ..... 36.7.1
Director of the Serious Fraud Office v. Airbus SE, 31 January 2020 (Case No.: U20200108); [2020] 1 WLUK 435 ..... 2.3.2, 3.3, 3.5.2.2, 3.5.2.4, 5.5, 7.4, 9.4.3, 9.4.5, 9.9.1, 12.7, 23.1, 23.2.1.2, 23.2.2.2, 3.4, 23.5.2, 25.16, 33.2.2, 46.2.1, 46.5, 46.7
Director of the Serious Fraud Office v. Airline Services Ltd, 30 October 2020 (Case No. U20201913) [2020] Southwark CC 2.3.2, 3.3, 23.2.1.2, 23.4, 25.16, 30.1, 46.2.1, 46.5
Director of the Serious Fraud Office v. Eurasian Natural Resources Corp [2018] EWCA Civ 2006; [2019] 1 WLR 791 ..... 1.3.1, 2.3.3, 2.3.6, 3.1, 3.2, 3.5.2.2, 7.11, 8.4, 9.4.7, 12.2, 12.4, 15.2.3, 17.3.6, 23.2.2.1, 23.2.4, 34.7.3, 36.2.4, 36.3.2.2,

© Law Business Research 2021

36.3.3, 36.4.1, 36.4.2, 36.4.3, 36.9.4
Dixons Stores Group v. Thames Television [1992] 1 All ER 349 ..... 36.6
Dormeuil Trade Mark [1983] RPC 131 ..... 36.3.2.1
Dorothy Gibson v. Pride Mobility Products Ltd [2017] CAT 9 ..... 34.3.5
Dougall. *See* R v. Dougall
Dubai Aluminium Co Ltd v. Al Alawi [1999] 1 WLR 1964 ..... 36.7.1
Dubai Bank v. Galadari (No. 6) Times, 22 April 1991 ..... 36.7.1
Duomatic Ltd, Re [1969] 2 Ch. 365; [1969] 2 WLR 114; (1968) 112 SJ 922 ..... 42.2.1.3, 42.2.1.4
Eclairs Group Ltd v. JKX Oil & Gas Plc [2015] UKSC 71; [2016] 3 All ER 641 ..... 42.2.1.2
ECU Group Plc v. HSBC Bank Plc [2018] EWHC 3045 ..... 34.7.3
EMW Law LLP v. Halborg [2017] EWHC 1014 (Ch) 36.5
ENRC v. Dechert. *See* Eurasian Natural Resources Corp v. Dechert
ENRC. *See* Director of the Serious Fraud Office v. Eurasian Natural Resources Corp
Environment Agency v. St Regis Paper Co Ltd [2012] 1 Cr App R 177 ..... 1.1.1, 9.3
Equitable Life Assurance Society v. Hyman [2002] 1 AC 408; [2000] 3 WLR 529; [2001] Lloyd's Rep. I.R. 99 ..... 42.2.1.4
Eurasian Natural Resources Corp litigation. *See* Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd
Eurasian Natural Resources Corp Ltd v. Dechert; sub nom. Dechert LLP v. Eurasian Natural Resources Corp Ltd [2016] EWCA Civ 375; [2016] 1 WLR 5027; [2017] 3 All ER 1084; [2016] 4 WLUK 393; [2016] CP Rep 31; [2016] 3 Costs LO 32736.8, 36.8.1, 36.9, 36.9.1, 36.9.2
Ex Parte Campbell. *See* Cathcart Ex p Campbell, Re
Fadairo v. Suit Supply UK Lime Street Ltd [2014] ICR D11 (EAT) 36.8.3
Financial Conduct Authority v. MS Amlin Underwriting Ltd [2020] EWHC 2448 (Comm) 34.3.4
Financial Conduct Authority v. MS Amlin Underwriting Ltd [2020] UKSC 2020/0177 ..... 34.3.4
Financial Conduct Authority v. Macris. *See* Macris v. Financial Conduct Authority
Financial Reporting Council Ltd v. Sports Direct International. *See* Sports Direct International Plc v. Financial Reporting Council
Financial Services Authority v. Amro International [2010] EWCA Civ 123 ..... 11.5.4
Financial Services Authority v. Anderson [2010] EWHC 308 (Ch) 34.2.1
Fofana v. Deputy Prosecutor Thubin Tribunal de Grande Instance de Meaux, France [2006] EWHC 744 (Admin) 1.2.1, 32.3.3
Ford v. FSA [2011] EWHC 2583 (Admin); [2012] EWHC 997 (Admin) 36.8.3
Foreign and Commonwealth Office (FCO) v. Bamieh (2019) EWCA Civ 803 ..... 19.3.4.5
Formica Ltd v. Export Credits Guarantee Department [1995] 1 Lloyd's Rep 692 ..... 36.5
Forster v. Friedland (CA, 10 November 1992) 36.6
Gamlen Chemical Co (UK) Ltd v. Rochem Ltd (No. 2) 7 December 1979 (CA) 36.7.1
GE Capital Corporate Finance Group v. Bankers Trust Co [1995] 1 WLR 172 ..... 36.9.3
General Accident Fire and Life Corp v. Tanter [1984] 1 WLR 100 ..... 36.8.2
General Mediterranean Holdings SA v. Patel [2000] 1 WLR 272 ..... 36.2.2, 36.7.2
Gillard v. Bates (1840) 6 M & W 547 ..... 36.2.1
Goddard v. Nationwide Building Society [1987] QB 670, CA 36.2.2
Gomez (Emilia) v. SSHD [2000] INLR 549 ..... 32.3.3
Gotha City v. Sotheby's (No1) [1998] 1 WLR 114, CA 2.3.3, 36.8, 36.8.1
Great Atlantic Insurance Co v. Home Insurance Co [1981] 1 WLR 529 ..... 36.8, 36.8.2
Greenough v. Gaskell (1833) 1 M&K 98 ..... 36.3.1
Guardian News and Media, In re [2010] UKSC 1; [2010] 2 AC 697 ..... 38.5.1.2
Guinness Peat Properties v. Fitzroy Robinson Partnership [1987] 1 WLR 1027 ..... 36.4.2

© Law Business Research 2021

Hajiyeva v. National Crime Agency; sub nom. National Crime Agency v. Hajiyeva [2020] EWCA Civ 108; [2020] 1 WLR 3209 ..... 28.3.2
Harmony Shipping v. Saudi Europe Line [1979] 1 WLR 1380, CA 36.2.5
Health and Safety Executive v. Paul Jukes. *See* R v. Jukes (Paul)
Hellenic Mutual War Risks Association (Bermuda) Ltd v. Harrison (The Sagheera) [1997] 1 Lloyd's Rep 160 ..... 36.4.2, 36.5
Henderson v. Dorset Healthcare University NHS Foundation Trust [2018] EWCA Civ 1841 34.6.1
Henderson v. Dorset Healthcare University NHS Foundation Trust UKSC 2018/0200 ..... 34.6.1
HH v. Deputy Prosecutor of the Italian Republic, Genoa. *See* R (on the application of HH) v. Westminster City Magistrates' Court
HH v. Italy. *See* R (on the application of HH) v. Westminster City Magistrates' Court
Highgrade Traders Ltd, Re [1984] BCLC 151 ..... 36.2, 36.4.1, 36.4.3
Hilton v. Barker Booth & Eastwood [2005] 1 WLR 567 ..... 36.2.1
HM Treasury v. Youssef, Al-Ghabra v. HM Treasury, Ahmed v. HM Treasury. *See* Guardian News and Media, In re
Hollington v. F Hewthorn & Co Ltd [1943] KB 587 ..... 34.7.1
Howard Smith Ltd v. Ampol Petroleum Ltd [1974] AC 821 ..... 42.2.1.2
Hunt (as Liquidator of System Building Services Group Ltd) v. Michie & Ors [2020] EWHC 54 (Ch) 42.2.1.2
Ibrahim v. HCA International Ltd [2019] EWCA Civ 2007 ..... 34.6.6
Iesini v. Westrip Holdings Ltd [2009] EWHC 2526 (Ch); [2010] BCC 420; [2011] 1 ..... 42.2.1.4
Innospec. *See* R v. Innospec Ltd
International Business Machines Corp v. Phoenix International (Computers) Ltd [1995] 1 All ER 413, 429 ..... 36.3.2.1
International Power Industries, Re [1985] BCLC 128 ..... 36.2.5
ISTIL Group Inc v. Zahoor [2003] 2 All ER 252 ..... 36.2.1
Item Software (UK) Ltd v. Fassihi [2004] EWCA Civ 1244 ..... 42.2.1.2
Ivey v. Genting Casinos (UK) Ltd t/a Crockfords [2017] UKSC 67 ..... 28.4, 30.1
JE Cade & Son Ltd, In re [1992] BCLC 213 ..... 34.4.2
Jedinak v. Czech Republic; sub nom. Jedinak v. District Court in Pardubice [2016] EWHC 3525 (Admin) 28.3.1
JLT Speciality Ltd, Final Notice, 19 December 2013 ..... 46.7
Joy v. Federation against Copyright Theft [1993] Crim LR 588 ..... 7.9
JSC BTA Bank v. Ablyazov [2014] EWHC 2788 (Comm) 36.7.1
JSC BTA Bank v. Ablyazov [2018] EWHC 1368 (Comm) 34.7.1
Kallakis v. AIB Group plc [2020] EWHC 460 (Comm) 34.4.1
Khuja v. Times Newspapers Limited [2017] UKSC 49; [2019] AC 161 ..... 38.5.1.1, 38.5.1.2, 38.5.2.1
Kuwait Airways Corp v. Iraqi Airways Corp (No. 6) [2005] 1 WLR 2734 ..... 36.7.1
L (A Minor) (Police Investigation: Privilege), Re [1997] AC 16 (HL) 36.2, 36.2.3, 36.4.2
Lambeth LBC v. Agoreyo [2019] EWCA Civ 322; [2019] ICR 1572 ..... 13.1.1.2
Lee v. SW Thames Health Authority [1985] 1 WLR 845, CA 36.2.5
Lennards Carrying Co and Asiatic Petroleum [1915] AC 705 ..... 7.5, 23.1
Levy v. Pope (1829) M & M 410 ..... 36.2.1
Lloyd v. Google LLC [2018] EWHC 2599 (QB) 34.6.7
LM v. London Borough of Lewisham [2009] UKUT 204 (AAC) 36.4.2
Lonsdale v. NatWest [2018] EWHC 1843 (QB) 3.4.1
Love v. Government of the United States [2018] EWHC 172 (Admin) 17.4.4.3, 32.5.1
Lyell v. Kennedy (No. 2) (1883) 23 Ch D 387 ..... 36.4.1
Lyell v. Kennedy (No. 3) (1884) 27 Ch D 1 ..... 36.3.2.2
MAC Hotels Ltd v. Rider Levett Bucknall UK Ltd [2010] EWHC 767 (TCC) 36.8.2

© Law Business Research 2021

Macfarlan v. Rolt (1872) LR 14 Eq 580 ..... 36.3.2.1
Macris v. Financial Conduct Authority; sub nom. Financial Conduct Authority v. Macris [2017] UKSC 19; [2015] EWCA Civ 490 ..... 17.6, 30.3
Mastercard case. *See* Walter Hugh Merricks CBE v. MasterCard Inc
MasterCard Incorporated and Others v. Walter Hugh Merricks CBE UKSC 2019/0118 ..... 34.3.5
Mayor and Corporation of Bristol v. Cox (1884) 26 Ch D 678 ..... 36.4.2
McE v. Prison Service of Northern Ireland [2009] 1 AC 908, HL 36.2.2, 36.7.1, 36.7.2
McKenzie. *See* R (on the application McKenzie) v. Director of the Serious Fraud Office
Meridian Global Funds Management Asia Ltd v. Securities Commission [1995] 2 AC 500 ..... 1.1.1, 9.3, 23.1
Mezey v. South West London & St George's Mental Health NHS Trust [2010] IRLR 512 ..... 13.1.1.2
Mid–East Sales v. Engineering & Trading Co PVT Ltd [2014] EWHC 892 (Comm) 36.8.2
Minter v. Priest [1930] AC 558 ..... 36.3.2.1
Mustad & Son v. Dosen [1964] 1 WLR 109 (Note) 36.8
National Crime Agency v. Azam [May 2015], District Court of Luxembourg; [2014] EWHC 4742 (QB) 28.3.2
National Crime Agency v. Mrs A [2018] EWHC 2534 (Admin) 28.3.2, 30.1.3
National Crime Agency v. Baker [2020] EWHC 822 (Admin); [2020] 4 WLUK 113 28.3.2, 30.1.3
National Crime Agency v. Hajiyeva. *See* Hajiyeva v. National Crime Agency
National Crime Agency v. Mansoor Hussain [2020] EWHC 432 (Admin) 28.3.2
National Crime Agency v. N [2017] EWCA Civ 253 ..... 3.4.1
National Grid Electricity Transmissions Plc v. ABB Ltd [2013] EWHC 822 (Ch) 12.6
Nationwide Building Society v. Various Solicitors (No. 1) [1999] PNLR 52 ..... 36.2.5
Nationwide Building Society v. Various Solicitors (No. 2) Times, 1 May 1988 ..... 36.2.5
Nea Karteria Maritime Co v. Atlantic & Great Lakes Steamship Corp (No. 2) [1981] Com LR 138 ..... 36.8.2
Nederlandse Reassurantie Groep Holding NV v. Bacon & Woodrow [1995] 1 All ER 976 .36.8.1
North West Anglia NHS Foundation Trust v. Gregg [2019] EWCA Civ 387 ..... 13.1.1.3
O'Rourke v. Darbishire [1920] AC 581 ..... 36.7.1
Oceanbulk Shipping & Trading SA v. TMT Asia [2011] 1 AC 662 ..... 36.6
Okhiria v. Royal Mail UKEAT/0054/14/LA 7.12
Omers Administration Corporation and others v. Tesco PLC [2019] EWHC 109 (Ch) 3.5.2.2, 28.2.2
Othman v. United Kingdom [2012] ECHR 56 ..... 32.3.5
Oxfordshire CC v. M [1994] Fam 151, CA 36.2.3
Panton v. Financial Institutions Services Ltd [2003] UKPC 95 ..... 34.2.1
Papachristos v. Serious Fraud Office; sub nom. Serious Fraud Office v. Papachristos [2014] EWCA Crim 1863 ..... 28.6.2
Paragon Finance v. Freshfields [1999] 1 WLR 1183 ..... 36.8, 36.8.2
Pascall v. Galinski [1970] 1 QB 38 ..... 36.2.1
Patel v. Mirza [2016] UKSC 42 ..... 34.6.1
PCP Capital Partners LLP v. Barclays Bank plc [2020] EWHC 1393 (Comm) 2.3.3, 23.2.2.1, 23.3.1, 23.5, 36.8.1, 36.8.2, 36.9.2
Pearce v. Foster (1885) 15 QBD 114 ..... 36.2.2, 36.2.3, 36.3.1
Pearse v. Pearse (1846) 1 De G & Sm 12 ..... 36.2.3
Perry v. SOCA. *See* Serious Organised Crime Agency v. Perry
PH v. Italy. *See* R (on the application of HH) v. Westminster City Magistrates' Court
Phoenix Contracts (Leicester) Ltd, Re [2010] EWHC 2375 (Ch) 42.2.1.2
PJSC Tatneft v. Bogolyubov [2020] EWHC 2437 (Comm) 36.3.2.1

© Law Business Research 2021

Practice Direction (CA (Crim Div): Costs in Criminal Proceedings) [2015] EWCA Crim 1568 ..... 25.6
Practice Direction (CA (Crim Div): Criminal Proceedings: General Matters) (Amendment No1) CA (Crim Div), 23 March 2016 [2016] EWCA Crim 97, [2016] 3 WLUK 678 ..... 25.6
Price Waterhouse (a firm) v. BCCI Holdings (Luxembourg) SA [1992] BCLC 583 ..... 36.4.3
Pride case. *See* Dorothy Gibson v. Pride Mobility Products Ltd
Prince Eze v. Conway [2019] EWCA Civ 88; [2019] 2 WLUK 34 ..... 34.6.1
Property Alliance Group Ltd v. Royal Bank of Scotland Plc [2015] EWHC 3187 (Ch); [2016] 1 WLR 992; [2015] 11 WLUK 108 ..... 34.7.3, 36.3.3
Property Alliance Group Ltd v. Royal Bank of Scotland Plc [2015] EWHC 1557 (Ch) 2.3.3, 12.4, 36.6, 36.8, 36.8.1
Property Alliance Group Ltd v. Royal Bank of Scotland Plc [2015] EWHC 3272 (Ch) 36.6
Queen on the Application of David Haigh v. City of Westminster Magistrates' Court [2017] EWHC 232 (Admin) 25.6
R (for and on behalf of the Health and Safety Executive) v. Paul Jukes. *See* R v. Jukes (Paul)
R (on the application of AL) v. Serious Fraud Office [2018] EWHC 856 (Admin) .. 1.3.1, 3.5.2.2, 7.4, 7.11, 9.4.7, 9.4.8, 9.7, 12.4, 13.4.1.2, 23.2.4, 36.3.2.2
R (on the application of Corner House) v. Director of the Serious Fraud Office [2008] EWHC 714 (Admin) 1.2.3
R (on the application of Energy Financing Team) v. Bow Street Magistrates' Court [2006] 1 WLR 1317 ..... 17.3.6
R (on the application of Gibson) v. Secretary of State for Justice [2018] UKSC 2 ..... 30.1.4
R (on the application of Guardian News and Media) v. City of Westminster Magistrates' Court [2012] EWCA Civ 420; [2013] QB 618 ..... 38.5.3
R (on the application of HH) v. Westminster City Magistrates' Court; sub nom. PH v. Italy, HH v. Italy (2012) 3 WLR 90 ..... 17.4.4.1
R (on the application of Howe) v. South Durham Magistrates Court [2005] RTR 4 ..... 36.2.1
R (on the application of Jet2.com Ltd) v. Civil Aviation Authority [2020] EWCA Civ 35; [2020] 2 WLR 1215 ..... 12.4, 36.3, 36.3.2.2, 36.3.3, 36.3.4, 36.8.2, 36.9.1
R (on the application of Jimenez) v. (1) First Tier Tax Tribunal and (2) Her Majesty's Commissioners for Revenue and Customs [2019] EWCA Civ 51; [2019] 1 WLR 2956; [2019] S.T.C. 746; [2019] 1 WLUK 315; 21 I.T.L. Rep. 561 ..... 11.5.2, 28.7
R (on the application of KBR Inc) v. Director of Serious Fraud Office [2018] EWHC 2012 (Admin) 9.9.4, 11.2.1, 17.3.7
R (on the application of KBR Inc) v. Director of the Serious Fraud Office [2018] EWHC 2368 (Admin); [2019] Lloyd's Rep FC 153 ..... 1.3.2, 5.6.4, 11.5.2, 28.1
R (on the application of Lord) v. Director of the Serious Fraud Office [2015] EWHC 865 (Admin) 15.3.3, 15.3.4
R (on the application of McKenzie) v. Director of the Serious Fraud Office [2016] EWHC 102 (Admin) 36.9.5
R (on the application of Miller Gardner) v. Minshull St Crown Court [2002] EWHC 3077 (Admin) 36.2.1
R (on the application of Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax [2003] 1 AC 563 HL 36.2.2, 36.7.2
R (on the application of PJSC Rosneft Oil Co) v. HM Treasury (C–72/15) EU:C:2017:236; [2018] QB 1; [2017] 3 WLR 1031; [2017] 3 WLUK 658; [2017] 3 CMLR 23; [2017] Lloyd's Rep FC 447 (GC) 28.5, 44.6.2

© Law Business Research 2021

R (on the application of Prudential Plc) v. Special Commissioner of Income Tax [2013] 2 AC 185, SC 36.3.2.1
R (on the application of Soma Oil and Gas Ltd) v. Director of the Serious Fraud Office [2016] EWHC 2471 (Admin) 3.5.2
R (on the application of Unaenergy Group Holdings Pte Ltd) v. Director of the Serious Fraud Office [2017] EWHC 600 (Admin) 9.9.4
R v. A Ltd, X, Y [2016] EWCA Crim 1469 ..... 1.1.1
R v. Alstom Network UK Ltd [2019] EWCA Crim 1318 ..... 46.7
R v. Andrews Weatherfoil [1972] 56 Cr App R 31 CA 7.5, 23.1
R v. Anjam Ahmed, Crown Court, (Southwark) 22 June 2010 ..... 9.5
R v. BAE Systems Plc [2010] EW Misc 16 (CC) 23.2.1.3
R v. Barclays PLC and Barclays Bank PLC [2018] (Southwark Crown Court) 9.3, 9.7, 23.1, 23.5
R v. Barton (David); R v. Booth (Rosemary) [2020] EWCA Crim 575, [2020] 4 All ER 742 ..... 28.4, 30.1
R v. Bayliss (Roy Alfred) (1994) 98 Cr App R 235 ..... 7.9
R v. Brown (Edward) [2016] 1 WLR 1141 ..... 36.7.1
R v. Central Criminal Court, Ex p. Francis and Francis [1989] AC 346, HL 36.2.5, 36.7.1
R v. Clifford [2014] EWCA Crim 2245 ..... 25.1
R v. Cox and Railton (1884) 14 QBD 153 ..... 36.7.1
R v. Creggy [2008] EWCA Crim 394 ..... 30.1.6
R v. Daniels [2010] EWCA Crim 2740 ..... 36.2.4
R v. Derby Magistrates' Court, Ex p. B [1996] AC 487 HL 36.2.2, 36.2.5
R v. Director of the Serious Fraud Office, Ex p. Saunders [1988] Crim LR 837 ..... 7.9
R v. Dougall [2010] EWCA Crim 1048 ..... 17.5, 23.1, 23.2.1.3, 30.1.1
R v. George Unreported, 7 December 2009 ..... 36.2.4
R v. Ghosh [1982] EWCA Crim 2 ..... 28.4
R v. Ghosh (Deb Baran) [1982] QB 1053 ..... 30.1
R v. Goodyear (Karl) [2005] EWCA Crim 888; [2005] 1 WLR 2532; [2005] 3 All ER 117; [2005] 4 WLUK 444; [2005] 2 Cr App R 20; [2006] 1 Cr App R (S.) 6; [2005] Crim LR 659 ..... 23.2.1.3, 25.4
R v. Gozutok and Brugge [2003] 2 CMLR 2 ..... 1.2.3
R v. Hall [2011] EWCA Crim 2753 ..... 25.1
R v. Harvey [2016] 4 All ER 521 ..... 25.3
R v. Hayes [2015] EWCA Crim 1944 ..... 30.1.1
R v. Inland Revenue Commissioners, Ex p. Lorimer [2000] STC 751 ..... 36.7.2
R v. Innospec Ltd [2010] 3 WLUK 784; [2010] Lloyd's Rep FC 462; [2010] Crim LR 665 ..... 3.5.2.4, 23.1, 23.2.1.1, 23.2.1.3, 23.5, 28.6.2, 33.2.2, 33.3
R v. Jukes (Paul); sub nom. Health and Safety Executive v. Jukes [2018] EWCA Crim 176; [2018] 1 WLUK 402; [2018] 2 Cr App R 9; [2018] Lloyd's Rep FC 157; [2018] Crim LR 658 ..... 7.11, 36.4.2
R v. Mason [1987] 3 All ER 481 ..... 15.4.2
R v. May (Raymond George) [2008] UKHL 28; [2008] 1 AC 1028 ..... 30.1.4
R v. Pabon [2018] EWCA Crim 420 ..... 28.4, 30.1
R v. Panel on Takeovers and Mergers, *Ex parte* Fayed [1992] BCC 524 ..... 34.2.1
R v. Papachristos & Kerrison, Unreported, Crown Court, (Southwark) 13 May 2013 ... 23.2.4, 36.8.2
R v. Peterborough Justices, Ex p. Hicks [1977] 1 WLR 1371 ..... 36.2.5, 36.3.1
R v. Rogers (Bradley) [2014] EWCA Crim 1680 ..... 28.3.1
R v. Sale [2013] EWCA Crim 1306 ..... 25.3
R v. Secretary of State for the Home Department, Ex p. Daly [2001] 2 AC 532, HL 36.7.2

© Law Business Research 2021

R v. Secretary of State for the Home Department, Ex p. Simms [2000] 2 AC 115, HL.....36.7.2
R v. Secretary of State for Transport Ex p. Factortame Ltd (1997) 9 Admin LR 591.....36.8.2
R v. Seelig [1992] 1 WLR 148.....7.9
R v. Skansen Interiors Ltd, Unreported.....3.3, 9.8, 46.2.1, 46.5, 46.7
R v. Smith [1994] 1 WLR 1396.....15.2.3
R v. Sweett Group Plc, Unreported.....7.4, 9.4.2, 9.7, 28.2.2, 46.2.1
R v. Tompkins (1977) 67 Cr App R 181.....36.2.2
R v. Turner (Elliott Vincent) [2013] EWCA Crim 643.....36.7.2
R v. Turner, Kerrison, Papachristos and Jennings in 2014.....28.6.2
R v. Twaites (Jacqueline Anne); R v. Brown (Derek Philip) (1991) 92 Cr App R 106 CA.....7.9, 15.2.3
R v. Underwood [2004] EWCA Crim 2256.....23.2.1.3
R v. Varley (John); R v. Jenkins (Roger); R v. Kalaris (Thomas); R v. Boath (Richard) [2019] EWCA Crim 1074; [2019] 6 WLUK 873.....23.1, 23.5
R v. Waya [2012] UKSC 51, [2012] 3 WLR 1188.....25.3, 30.1.4
R v. Welcher [2007] EWCA Crim 480; [2007] 3 WLUK 62; [2007] 2 Cr App R (S.) 83; [2007] Crim LR 804.....7.9, 15.2.3
Raiffeisen Bank International v. Asia Coal Energy Ventures Ltd [2020] 1 WLR 2298 36.7.2, 36.8
Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig [2017] All ER (D) 24442.2.1.4
Rawlinson & Hunter Trustees SA v. Akers. *See* Tchenguiz v. Director of the Serious Fraud Office (Non–Party Disclosure)
Rawlinson & Hunter Trustees SA v. Director of the Serious Fraud Office. *See* Tchenguiz v. Director of the Serious Fraud Office (Non–Party Disclosure)
RBS (Rights Issue Litigation), Re [2016] EWHC 3161 (Ch).....2.3.3, 2.3.6, 7.11, 9.4.7, 34.5, 34.7.3, 36.3.2.2, 36.9, 36.9.1, 36.9.4
Reed Executive plc v. Reed Business Information Ltd [2004] 1 WLR 3026.....36.6
Revenue and Customs Commissioners v. Holland [2010] UKSC 51.....25.7
Richard v. BBC [2018] EWHC 1837 (Ch); [2019] Ch 169.....17.6, 38.5.1.2
Robert Hitchins Ltd v. International Computers Ltd (10 December 1996, CA).....36.2.3, 36.5
Rogers v. Hoyle [2014] EWCA Civ 257.....34.7.1
Rolls-Royce case. *See* Serious Fraud Office v. Rolls-Royce Plc
Saunders v. United Kingdom [1996] ECHR 65.....17.3.5
Saxton (Deceased), Re [1962] 1 WLR 968.....36.2.3
Sayers v. Clarke Walker [2002] EWHC Ch 60.....36.2.4
Schneider v. Leigh [1955] 2 QB 195.....36.2.5
Scott v. Government of the United States of America [2018] EWHC 2021 (Admin) .. 17.4.4.3, 32.5.1
Scott v. Scott [1913] AC 417.....38.5.1.2
Scottish Lion Insurance Co Ltd v. Goodrich Corp [2011] CSIH 18.....36.8.1
Secretary of State for Health v. Servier Laboratories; National Grid Electricity Transmission Plc v. ABB [2013] EWCA Civ 1234; [2014] 1 WLR 4383; [2013] 10 WLUK 642; [2014] UKCLR 263; [2014] Lloyd's Rep FC 175.....12.6
Secretary of State for Trade & Industry v. Baker [1998] Ch 356.....36.2.3
Serious Fraud Office v. Airbus SE. *See* Director of Serious Fraud Office v. Airbus
Serious Fraud Office v. Akle [2020] at Southwark Crown Court.....11.5.1
Serious Fraud Office v. Barclays PLC & ANR [2018] EWHC 3055 (QB); [2020] 1 Cr App R 28.....1.1.1, 9.3, 9.7, 23.1, 23.5
Serious Fraud Office v. Bittar and Moryoussef, Crown Court (Southwark), 19 July 2018 .....30.1.1

© Law Business Research 2021

Serious Fraud Office v. Depuy International Ltd, Unreported 1.2.1
Serious Fraud Office v. G4S Care and Justice Services (UK) Limited, 17 July 2020, Case No. U20201392, [2020] 7 WLUK 303 ..... 1.1.1, 1.3.4, 2.3.2, 3.3, 3.5.2.4, 7.4, 7.11, 9.5, 23.1, 23.2.1.2, 23.3.2, 23.4, 25.16, 30.1, 33.2.2, 46.4.1.5, 46.5
Serious Fraud Office v. Guralp Systems Ltd, 22 October 2019, Case No. U20190840, [2020] Lloyd's Rep FC 90 ..... 2.3.2, 3.3, 5.5, 7.3, 23.1, 23.2.1.2, 23.4, 25.16, 27.6, 46.2.1
Serious Fraud Office v. Hall (Bruce), Crown Court (Southwark), 22 July 2014 . 23.2.1.1, 23.5, 30.1.1
Serious Fraud Office v. Karimova [2020] 6 WLUK 383 ..... 28.3.2
Serious Fraud Office v. Papachristos and Kerrison. *See* Papachristos v. Serious Fraud Office
Serious Fraud Office v. Rolls-Royce Plc and Rolls-Royce Energy Systems Inc (Case No. U20170036) [2017] 1 WLUK 189; [2017] Lloyd's Rep FC 249.. 1.1.1, 2.3.2, 3.2, 3.3, 3.5.2.3, 3.5.2.4, 5.5, 7.4, 9.4.2, 9.4.3, 9.4.5, 9.4.6, 9.4.7, 9.5, 12.7, 23.1, 23.2.1.2, 23.2.2.2, 23.4, 25.16, 27.2, 30.1, 33.5.2, 36.2.4
Serious Fraud Office v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc, Crown Court (Southwark), 17 January 2017 ..... 46.2.1, 46.5, 46.7
Serious Fraud Office v. Saleh [2018] EWHC 1012 (QB) 25.8
Serious Fraud Office v. Serco Geografix Ltd (Case No.: U20190413) [2019] 7 WLUK 45; [2019] Lloyd's Rep FC 518; [2020] Crim LR 66 CC 1.1.1, 2.3.2, 3.3, 3.5.2.4, 5.2, 5.5, 7.3, 23.2.1.2, 23.4, 25.16, 30.1, 33.2.2, 33.5.2, 46.7
Serious Fraud Office v. Sarclad Ltd. *See* Serious Fraud Office v. XYZ Ltd
Serious Fraud Office v. Standard Bank Plc (now ICBC Standard Bank Plc) (Final) (Case No. U20150854) [2015] 11 WLUK 804; [2016] Lloyd's Rep FC 102 ..... 2.3.2, 3.4.1, 3.5.2.4, 5.2, 7.4, 7.11, 9.4.3, 9.4.5, 9.7, 23.1, 23.2.1.2, 23.2.2.2, 23.4, 25.16, 33.2.2, 46.2.1
Serious Fraud Office v. Tesco Stores Ltd (Case No. U20170287) [2017] 4 WLUK 558; [2019] Lloyd's Rep FC 283 ..... 1.1.1, 2.3.2, 3.2, 3.5.2.4, 5.2, 23.2.1.2, 23.4, 25.16, 27.6, 46.5, 46.7
Serious Fraud Office v. Tesco Stores Ltd (Case No. U20170287) [2017] EW Misc 30 (CrownC) 3.2, 23.2.1.2, 23.4
Serious Fraud Office v. Tesco Stores Ltd (Case No. U20170287) [2019] EW Misc 1 (CrownC) 17.5
Serious Fraud Office v. XYZ Ltd (now known to be Sarclad Ltd) [2016] Lloyd's Rep FC 517, [2016] 7 WLUK 211 (Case No. U20150856) 1.1.1, 23.1, 23.2.1.2, 46.2.1, 46.5
Serious Fraud Office v. XYZ Ltd (now known to be Sarclad Ltd) [2016] Lloyd's Rep FC 509, [2016] 7 WLUK 220 ..... 1.1.1, 3.5.1.1, 3.5.2.2, 3.5.2.4, 7.4, 7.11, 9.4.3, 9.4.5, 17.5, 23.1, 23.2.1.2, 23.2.4, 23.3.2, 23.4, 25.16
Serious Fraud Office v. XYZ Ltd (now known to be Sarclad Ltd) (Case No. U20150856) Unreported, 24 June 2016 ..... 2.3.2, 3.5.1.1, 7.4, 9.4.5, 33.2.2
Serious Organised Crime Agency v. Perry; sub nom. Perry v. Serious Organised Crime Agency [2012] UKSC 35 ..... 28.3.2
Shankaran v. India (2014) EWHC 957 (Admin) 17.4.4.1

© Law Business Research 2021

Singularis Holdings Ltd (In Official Liquidation) (A Company Incorporated in the Cayman Islands) v. Daiwa Capital Markets Europe Limited [2019] UKSC 50 ..... 3.5.1.2
SL Claimants v. Tesco Plc [2019] EWHC 3315 (Ch) 36.8
Soering v. United Kingdom (1989) 11 EHRR 439 ..... 17.4.4.1
Somatra v. Sinclair Roche & Temperley [2000] 1 WLR 2453 ..... 36.6
Southwark and Vauxhall Water Co v. Quick (1878) 3 QBD 315 ..... 36.4.1
Sports Direct International Plc v. Financial Reporting Council [2020] EWCA Civ 177; [2020] 2 WLR 1256 ..... 36.3.1, 36.3.4, 36.7.2, 36.8.1
St Regis case. *See* Environment Agency v. St Regis Paper Co Ltd
Standard Bank Plc. *See* Serious Fraud Office v. Standard Bank Plc
Stephen Robert Allen v. Financial Conduct Authority [2014] UKUT 0348 (TCC) 34.7.2
Stoffel & Co v. Grondona [2020] UKSC 42 ..... 34.6.1
Sulaiman v. France [2016] EWHC 2868 (Admin) 28.3.1
Sumitomo Corp v. Credit Lyonnais Rouse Ltd [2002] 1 WLR 479, CA 36.2.3
Svenska Handelsbanken v. Sun Alliance and London Insurance plc [1995] 2 Lloyd's Rep 84 ..36.5
Sweett Group Plc case. *See* R v. Sweett Group Plc
TAG Group Litigation. *See* Winterthur Swiss Insurance Co v. AG (Manchester) Ltd (In Liquidation)
Taylor v. Forster (1825) 2 C&P 195 ..... 36.3.2.1
Taylor Goodchild Ltd v. Taylor [2020] EWHC 2000 (Ch) 34.4.2
Tchenguiz v. Director of the Serious Fraud Office (Non–Party Disclosure); sub nom. Rawlinson and Hunter Trustees SA v. Akers [2014] EWCA Civ 136 ..... 23.2.4, 36.4.2, 36.4.3
Tchenguiz v. Director of the Serious Fraud Office; sub nom. Rawlinson & Hunter Trustees SA v. Director of the Serious Fraud Office [2014] EWCA Civ 1129 ..... 36.4.3, 36.8.3
Tchenguiz v. Grant Thornton [2017] EWHC 310 (Comm) 34.7.3
Tesco Stores v. Brent LBC [1993] 1 WLR 1037; [1993] 2 All ER 718 ..... 9.3
Tesco Stores Ltd v. Office of Fair Trading [2012] CAT 6 ..... 36.4.2
Tesco Supermarkets Ltd v. Nattrass [1972] AC 153; [1971] 2 WLR 1166; [1971] 2 All ER 127; [1971] 3 WLUK 144; 69 LGR 403; (1971) 115 SJ 285 ..... 1.1.1, 7.5, 9.3, 15.2.1, 23.1
Three Rivers DC v. Bank of England [2001] UKHL 16 ..... 9.4.7
Three Rivers DC v. Bank of England (Three Rivers No. 5) [2003] EWCA Civ 474; [2003] QB 1556 ..... 3.5.2.2, 7.11, 9.4.7, 23.2.4, 36.3.1, 36.3.2.1, 36.3.2.2, 36.4.1, 36.4.3, 36.9.1
Three Rivers DC v. Bank of England (No. 6) [2005] 1 AC 610, HL 3.5.2.2, 12.4, 36.2, 36.2.1, 36.2.2, 36.2.3, 36.2.4, 36.3, 36.3.1, 36.3.2.2, 36.3.3, 36.4.1, 36.4.2
Timis and another v. Osipov [2018] EWCA Civ 2321 ..... 19.2.1.4
Trade Practices Commission v. Sterling (1979) 36 FLR 244 ..... 36.3.2.2
Treacy v. DPP [1971] AC 537 ..... 23.1
Twaites and Brown. *See* R v. Twaites (Jacqueline Anne); R v. Brown (Derek Philip)
Unaoil case. *See* Serious Fraud Office v. Akle
UK Trucks Claim Limited v. Fiat Chrysler Automobiles N.V. and Others (pending) 34.3.5
Unilever plc v. Procter & Gamble Co [2000] 1 WLR 2436, 2444-5 (CA) 36.6
United States v. Philip Morris Inc (No. 1) [2004] EWCA Civ 330, CA 36.4.2
USP Strategies plc v. London General Holdings Ltd [2004] EWHC 373 (Ch) 36.3.1, 36.5, 36.8, 36.8.1
Ventouris v. Mountain [1991] 1 WLR 607 ..... 36.3.1, 36.3.2.2, 36.7.1
Vincent Brown aka Vincent Bajinja, et al. v. Government of Rwanda, Secretary of State for the Home Department (2009) EWHC 770 (Admin) 17.4.4.1

© Law Business Research 2021

Visx Inc v. Nidex [1999] FSR 91 ..... 36.2.3
Walker v. Wilsher (1889) 23 QBD 335 ..... 36.6
Walter Hugh Merricks CBE v. MasterCard Incorporated [2017] CAT 16 ..... 34.3.5
Walter Hugh Merricks CBE v. MasterCard Incorporated [2019] EWCA Civ 674 ..... 34.3.5
Waugh v. British Railways Board [1980] AC 521 HL 36.2, 36.2.3, 36.4, 36.4.3
Wentworth v. Lloyd (1864) 10 HLC 589 ..... 36.2.4
West London Pipeline v. Total UK [2008] 2 CLC 258 ..... 36.9.3, 36.9.4
WH Holding Limited and West Ham United Football Club Ltd v. E20 Stadium LLP [2018] EWCA Civ 2652 ..... 36.4.3, 36.9.3, 36.9.4
Wheeler v. Le Marchant (1881) 17 Ch D 675, CA 36.3.2.1
Wilden Pump Engineering Co v. Fusfield [1985] FSR 159, CA 36.3.2.1
William Hill Organisation Ltd v. Tucker [1998] IRLR 313 ..... 13.1.1.1
Winterthur Swiss Insurance Co v. AG (Manchester) Ltd (In Liquidation) [2006] EWHC 839 (Comm) (TAG Group Litigation) 36.5
Wm Morrison Supermarkets Plc v. Various Claimants [2020] UKSC 12 ..... 34.6.7
Wood v. Commercial First Bank Ltd (in Liquidation) [2019] EWHC 2205 (Ch) 34.6.1
Woodward v. Abbey National Plc (2006) EWCA Civ 822 ..... 19.2.1.1
ZXC v. Bloomberg LP [2020] EWCA Civ 611 ..... 17.6, 38.5.1.2

United States

3Com Corp. v. Diamond II Holdings, Inc., No. 3933–VCN, 2010 Del. Ch. LEXIS 126 (Ch. 31 May 2010) 2.3.3
7 W. 57th St. Realty Co., LLC v. Citigroup, Inc., 2015 WL 1514539, at *1 n.1 (S.D.N.Y. 31 March 2015), aff'd, 771 F. App'x 498 (2d Cir. 2019) 24.5.4
100Reporters LLC v. US Department of Justice, No. 14–1264–RC (D.D.C. 31 March 2017) 33.5.5
100Reporters LLC v. US Department of Justice, 316 F. Supp. 3d 124 (D.D.C. 2018) 24.5.2
ABF Capital Management v. Askin Capital, 2000 WL 191698 (S.D.N.Y. 10 February 2000) 24.3.1
ABN AMRO Bank N.V, In re, (Department of Justice 9 May 2010) 24.4.1
Absolute Activist Value Master Fund Ltd. v. Ficeto, 677 F.3d 60, 68–69 (2d Cir. 2012) 29.2.2
Ahmad v. Wigen, 910 F.2d 1063, 1065 (2d Cir. 1990) 18.3.5
Alaska Electrical Pension Fund v. Bank of America Corp., 2017 WL 280816 (S.D.N.Y. 20 January 2017) 24.3.1, 37.4
Alexander v. United States, 509 U.S. 544 (1993) 31.2.5.2
Atl. Specialty Ins. Co. v. Midwest Crane Repair, LLC, 2020 WL 5118067, at *3 (D. Kan. 31 August 2020) 35.3.1.2
Ambac Assurance Corp. v. Countrywide Home Loans, Inc., 27 N.Y.3d 616, 627 to 629 (2016) 2.3.3, 35.5.3
Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011) 41.5.3
Anthem, Inc. Data Breach Litig., In re, 162 F. Supp. 3d 953, 970 (N.D. Cal. 2016) 41.5.3
Anthony Menendez v. Halliburton, Inc., 2011 WL 4915750 (ARB 13 September 2011) 20.2.3
Antitrust Grand Jury, In re, 805 F.2d 155 (6th Cir. 1986) 37.1.1.1
Arizona v. Washington, 434 U.S. 497 (1978) 39.3.1
Aronson v. Lewis, 473 A.2d 405 (Del. 1984) 35.3.2.2
Aronson v. Lewis, 473 A.2d 805 (Del. 1984) 43.3.2
Arthur Andersen LLP v. United States, 544 U.S. 696 (2005) 1.1.2
Artukovic v. Rison, 784 F.2d 1354, 1356 (9th Cir. 1986) 18.3.2
Asadi v. GE Energy (USA), LLC, No. 4:12–345, 2012 WL 2522599 (S.D. Tex. 28 June 2012) 20.2.3

© Law Business Research 2021

Ashmore v. CGI Group Inc., 138 F. Supp. 3d 329 (S.D.N.Y. 2015) 2.3.4
AT&T Mobility v. Concepcion, 563 U.S. 333 (2011) 35.3.1.5
Austin v. United States, 509 U.S. 602 (1993) 31.2.5.2
A-Valey Engineers, Inc. v. Bd. of Chosen Freeholders of Cty. of Camden, 106 F. Supp. 2d 711, 713 (D.N.J. 2000) 35.3.3.2
Babbitt v. Sweet Home Chapter of Communities for a Greater Oregon, 515 U.S. 687, 704 n.18 (1995) 29.3
Banneker Ventures, LLC v. Graham, Civil Action No. 13-391 (RMC), 2017 WL 2124388, at *1-*2,*4-*5 (D.D.C. 16 May 2017) 37.1.2
Barclays Bank Plc, In re, (Department of Justice 16 August 2010) 24.4.1
Barnes v. Andrews, 298 F. 614, 615 (S.D.N.Y. 1924) 43.2.1
Bascuñán v. Elsaca, 927 F.3d 108 (2d Cir. 2019) 29.5
Baxter v. Palmigiano, 425 U.S. 308, 318 (1976) 35.2.2
Bear Stearns Mortg. Pass-Through Certificates Litigation, In re, 851 F. Supp. 2d 746 (S.D.N.Y. 2012) 24.5.4
Bevill, Bresler & Schulman Asset Management Corp., In re, 805 F.2d 120 (3d Cir. 1986) 14,8, 37.1.3, 37.2
Blackledge v. Perry, 417 U.S. 21 (1974) 31.1.1
Blech Sec. Litigation, In re, 2003 U.S. Dist. LEXIS 4650 (S.D.N.Y. 26 March 2003) 35.4.1
Bohach v. City of Reno, 932 F. Supp. 1232 (D Nev. 1996) 40.3
Bordenkircher v. Hayes, 434 U.S. 357 (1978) 31.1.1
Bottaro v. Hatton Assocs, 96 F.R.D. 158 (E.D.N.Y. 1982) 24.3.1
Bowers v. NCAA, 563 F. Supp. 2d 508 (D.N.J. 2008) 35.4.1
Braswell v. United States, 487 U.S. 99, 102 (1988) 18.5.3, 35.2.2
Breed v. Jones, 421 U.S. 519 (1975) 1.2.2
Brown v. Trigg, 791 F.2d 598 (7th Cir. 1986) 37.7
Bushmaker v. A. W. Chesterton Co, No. 09–CV–726–SLC, 2013 WL 11079371 (W.D. Wis. 1 March 2013) 39.1.3
Buttonwood Tree Value Partners, L.P. v. R.L. Polk & Co, Inc., Civil Action No. 9250–VCG, 2018 WL 346036 (Del. Ch. 10 January 2018) 37.1.1.2
Cadence Pharm., Inc. v. Fresenius Kabi USA, LLC, 996 F. Supp. 2d 1015, 1019 (S.D. Cal. 2014) 18.5.1
Calvin Klein Trademark Trust v. Wachner, 198 F.R.D. 53 (S.D.N.Y. 2000) 37.7
Caremark Int'l Inc. Derivative Litig., In re, 698 A.2d 959, 967 (Del. Ch. 1996) 43.2.1, 43.2.2, 43.2.3, 43.3.1, 43.6
Carpenters Health & Welfare Fund v. Coca–Cola Co, 2008 U.S. Dist. LEXIS 112503 (N.D. Ga. 23 April 2008) 35.4.1
Carpenters Pension Tr. Fund of St. Louis, St. Clair Shores Police & Fire Ret. Sys. v. Barclays PLC, 56 F. Supp. 3d 549, 552 n.3 (S.D.N.Y. 2014) 24.5.4
Carter v. Welles-Bowen Realty, Inc., 736 F.3d 722, 727 (6th Cir. 2013) 29.3
Cathode Ray Tube (CRT) Antitrust Litigation, In re, 2014 WL 1247770 (N.D. Cal. Mar. 26 2014) 40.5
CE Harris, Inc. v. Int'l Bhd. of Elec. Workers Local 595, 2013 WL 6252485, at *5 (N.D. Cal. 3 December 2013) 35.2.2
Charlton v. Kelly, 229 U.S. 447, 462 (1913) 18.3.4
Chevron Corp. v. Pennzoil Co, 974 F.2d 1156 (9th Cir. 1992) 37.1.1.1, 37.7.1
Cinerama, Inc. v. Technicolor, Inc., 663 A.2d 1156, 1166 (Del. 1995) 43.3.1
Citibank, N.A, In the Matter of, CFTC Docket No. 16–16 (25 May 2016) 24.5.4
Citigroup. *See* Securities and Exchange Commission v. Citigroup Global Markets, Inc.

© Law Business Research 2021

City of Pontiac General Employees' Retirement System v. Wal–Mart Stores Inc., et al, Case No. 5:12–cv–5162 (W.D. Ark 2012), Order 5 May 2017 ..... 2.3.3
City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG, 752 F.3d 173, 179–80 (2d Cir. 2014) 29.2.2
Clark Equip. Co v. Lift Parts Mfg Co, No. 82 C 4585, 1985 WL 2917 (N.D. Ill. 1 Oct. 1985) 37.3.2
Clark v. City of Munster, 115 F.R.D. 609 (N.D. Ind. 1987) 37.7
Clark v. United States, 289 U.S. 1 (1933) 37.1.1.1
Closed Joint Stock Co. 'CTC Network' v. Actava TV, Inc., 2016 WL 1364942, at *5 (S.D.N.Y. 28 March 2016) 35.4.3
Collins v. Loisel, 262 U.S. 426, 429 (1923) 18.3.5
Collins v. Loisel (Collins II), 259 U.S. 309, 317 (1922) 18.3.2
Collins v. Miller, 252 U.S. 364, 369 (1920) 18.3.5
Columbia/HCA Healthcare Corp. Billing Practices Litigation, In re, 293 F.3d 289 (6th Cir. 2002) 12.4, 37.5
Commodity Futures Trading Commission v. Deutsche Bank AG, 2016 WL 6135664 (S.D.N.Y. 20 October 2016) 24.4.1
Commodity Futures Trading Commission v. Newell, 301 F.R.D. 348 (N.D. Ill. 2014) 37.8
Commodity Futures Trading Commission v. Vision Fin. Partners, LLC, 19 F. Supp. 3d 1126, 1131 (S.D. Fla. 2016) 29.6
Commodity Futures Trading Commission v. Weintraub, 471 U.S. 343 (1985) 37.2
Conopco, Inc. v. Wein, 2007 WL 1040676 (S.D.N.Y. 4 April 2007) 24.3.1
Cooke v. Oolie, Civ. Action No. 11134, 2000 Del. Ch. LEXIS 89, at *58–59 (Del. Ch. 24 May 2000) 43.2.1
Coordinated Pretrial Proceedings in Petroleum Prod. Antitrust Litigation, In re, 658 F.2d 1355 (9th Cir. 1981) 37.3.2
Copper Market Antitrust Litigation, In re, 200 F.R.D. 213 (S.D.N.Y. 2001) 37.7
Creel v. Ecolab, Inc., 2018 WL 5733382, at *5 (Del. Ch. 31 October 2018) 35.3.2.3
Cyan Inc. v. Beaver Cnty. Employees Retirement Fund, 138 S. Ct. 1061 (2018) 35.3.1.4
Dallas Airmotive, Inc., In re, (Department of Justice 10 December 2014) 24.4.1
Davis v. City of New York, No. 10 Civ. 0699 (S.D.N.Y. 28 April 2015) 33.1
Day v. Staples, Inc., 555 F.3d 42 (1st Cir. 2009) 2.3.4
Dellwood Farms, Inc. v. Cargill, Inc., 128 F.3d 1122 (7th Cir. 1997) 37.5
Depuy Orthopaedics, Inc. Pinnacle Hip Implant Prod. Liab. Litigation, In re, No. 11 MD 2244, 2013 WL 2091715 (N.D. Tex. 15 May 2013) 33.5.5
Descoteaux v. Mierzwinski (1982) 141 DLR (3d) 590 ..... 36.3.2.1
Digital Realty Trust, Inc. v. Somers, 138 S. Ct. 767 (2018) 14.2, 20.1.1, 20.3.1
Dimas–Martinez v. State, 385 S.W.3d 238 (Ark. 2011) 39.2.2
DirecTV v. Imburgia, 136 S. Ct. 463 (2015) 35.3.1.5
Diversified Industries Inc. v. Meredith, 572 F.2d 596 (8th Cir. 1977) (en banc) 37.5
Doe v. Indyke, 2020 WL 5518384, at *6 (S.D.N.Y. 14 September 2020) 35.2.1
Doe v. Kohn Nast & Graf, 866 F. Supp. 190 (E.D. Pa. 1994) 40.3
Drummond Co v. Conrad & Scherer, LLP, 885 F.3d 1324 (11th Cir. 2018) 37.1.1.1
Duling v. Gristede's Operating Corp., 266 F.R.D. 66, 77 (S.D.N.Y. 2010) 35.4.3
Durling v. Papa John's International, Inc., No. 16 Civ. 3592 (CS) (JCM), 2018 U.S. Dist. LEXIS 11584 (S.D.N.Y. 24 January 2018) 37.7
Edwards v. Arthur Andersen LLP 44, Cal. 4th 937 (2008) 14.6.2.2
EM Ltd. v. Republic of Argentina, 695 F.3d 201, 207 (2d Cir. 2012) 35.4.3
Epic Sys. Corp. v. Lewis, 138 S. Ct. 1612 (2018) 35.3.1.5

© Law Business Research 2021

Equal Employment Opportunity Commission v. Arabian Am. Oil Co (Aramco), 499 U.S. 244 (1991) 29.3
Erickson v. Hocking Technical College, Case No. 2:17–cv–360, 2018 U.S. Dist. LEXIS 50075 (S.D. Ohio 27 March 2018) 37.3.1
Estes v. State of Tex, 381 U.S. 532 (1965) 39.1.1
European Community v. RJR Nabisco, Inc., 764 F.3d 129 (2d Cir. 2014) rev'd on other grounds, 136 S. Ct. 2090 (2016) 29.5
Export–Import Bank of the U.S. v. Asia Pulp & Paper Co, 232 F.R.D. 103 (S.D.N.Y. 2005) ..37.7
Extradition of Chan Seong-I, In re, 346 F. Supp. 2d 1149, 1157 (D.N.M. 2004) 18.3.4
Extradition of Tafoya, In re, 572 F. Supp. 95, 97 (W.D. Tex. 1983) 18.3.5
Fannie Mae 2008 Sec. Litig., In re, 891 F. Supp. 2d 458, 471 (S.D.N.Y. 2012), aff'd, 525 F. App'x 16 (2d Cir. 2013) 24.5.4
F Hoffman–LaRoche Ltd v. Empagran S.A, 542 US 155 (2004) 29.7
Federal Communications Commission v. Am. Broadcast Co., 347 U.S. 284, 296 (1954) 29.3
Federal Trade Commission v. GlaxoSmithKline, 294 F.3d 141 (D.C. Cir. 2002) 37.7
Feldman v. Law Enf 't Assocs. Corp., 752 F.3d 339 (4th Cir. 2014) 20.1.1, 20.2.3
Fluor Intercontinental, Inc., In re, 803 Fed. Appx. 697, 701-702 (4th Cir. 2 March 2020) 37.5
Flynn, In re, 961 F.3d 1215, 1220 (D.C. Cir. 2020); sub nom. In re: Michael T. Flynn, 2020 WL 4355389 (D.C. Cir. 30 July 30 2020) 24.4.1
Francis v. United Jersey Bank, 432 A.2d 814, 822 (N.J. 1981) 43.2.1
Franklin's Budget Car Sales, Inc., In re, File No. 102-3094, No. C-4371 (F.T.C. 3 October 2012), 2012 WL 5375157 ..... 41.5.3
Fraser v. Fiduciary Trust Co Int'l, No. 04 CIV. 6958 (PAC), 2009 WL 2601389 (S.D.N.Y. 25 August 2009) aff'd, 396 F. App'x 734 (2d Cir. 2010) 20.2.3
Fraser v. Nationwide Mut. Ins. Co, 352 F.3d 107 (3d Cir. 2003) 40.3
Friedman v. Bache Halsey Stuart Shields, Inc., 738 F.2d 1336 (D.C. Cir. 2009) 35.3.1.2
FrontPoint Asian Event Driven Fund, L.P. v. Citibank, N.A, No. 16 CIV. 5263 (AKH), 2017 WL 3600425 (S.D.N.Y. 18 August 2017) 29.5
FTC v. EMA Nationwide, Inc., 767 F.3d 611, 627 (6th Cir. 8 September 2014) 35.2.1
FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245 (3d Cir. 2015) 41.5.3
Funke v. Federal Express Corp., ARB No. 09–004, ALJ No. 2007–SOX–043 (ARB 8 July 2011) 20.1.1
G–I Holdings, Inc., In re, 218 F.R.D. 428 (D.N.J. 2003) 37.7
Galvin v. Pepe, No. 09–cv–104–PB, 2010 WL 3092640 (D.N.H. 5 August 2010) 37.8
Gamble v. United States, 139 S. Ct. 1960 (2019) 1.2.2
Gantler v. Stephens, 965 A.2d 695, 705–06 (Del. 2006) 43.3.2
Garner v. Wolfinbarger 430 F.2d 1093 (5th Cir. 1970), cert. denied, 401 U.S. 974, 91 S. Ct. 1991, 28 L.Ed.2d 323 (1971) 6.3, 37.1.1.2
Garrett v. Garden City Hotel, Inc., No. 05–CV–0962, 2007 WL 1174891 (E.D.N.Y. 19 April 2007) 20.2.3
Garrity v. John Hancock Mutual Life Ins. Co, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 7 May 2002) 40.3
Garrity v. New Jersey, 385 U.S. 493 (1967) 18.4.2.2, 37.3.1
Geders v. United States, 425 U.S. 80 (1976) 39.1.3
Genberg v. Porter, 882 F.3d 1249, 1255 (10th Cir. 2018) 20.1.1
General Cable Corp., In re, (Department of Justice 22 December 2016) 24.4.1
General Motors LLC Ignition Switch Litigation, In re, 2015 WL 7769524 (S.D.N.Y. 30 November 2015) 24.3.1, 24.5.4
General Motors LLC Ignition Switch Litigation, In re, 80 F. Supp. 3d 521 (S.D.N.Y. 2015) 11.5, 37.3.1

© Law Business Research 2021

General Motors LLC Ignition Switch Litigation, In re, 2016 WL 4410008, at *5 (S.D.N.Y. 18 August 2016) 24.3.1, 24.5.4
Gentile v. State Bar of Nevada, 501 U.S. 1030 (1991) 39.1.1, 39.3.2
Gerstein v. Pugh, 420 U.S. 103, 117 n.19 (1975) 18.6
Gilman v. Marsh & McLennan Co, Inc., 826 F.3d 69 (2d Cir. 2016) 14.1, 16.3.1
Giunta v. Dingman, 893 F.3d 73, 82 (2d Cir. 2018) 29.2.2
GMR Transcription Servs., Inc., In re, FTC File No. 122-3095, No. C-4482 (F.T.C. Feb. 3, 2014), 2014 WL 492352 ..... 41.5.3
Goldman Sachs Grp, Inc. Sec. Litigation, In re, No. 1:10–cv–03461–PAC, 2015 WL 5613150 (S.D.N.Y. 6 April 2015) 24.2
Gonzalez, In re, 217 F. Supp. 717, 720 (S.D.N.Y. 1963) 18.3.5
Gorman–Bakos v. Cornell Coop. Extension, 252 F.3d 545 (2d Cir. 2001) 20.2.3
Grand Jury Investigation, In re, 772 N.E.2d 9 (Mass. 2002) 37.1.1.1
Grand Jury Investigation, In re, No. 17–2336, 2017 WL 4898143 (D. D.C, 2 October 2017) 37.5
Grand Jury Investigation, In re, No. 19-15, 2019 WL 217916, *13 (D. D.C. 4 March 2019) 37.3.1
Grand Jury Proceeding, In re, 691 F.2d 1384 (11th Cir. 1982) 29.11
Grand Jury Proceedings, In re, 102 F.3d 748 (4th Cir. 1996) 37.1.1.1
Grand Jury Proceedings, In re, 219 F.3d 175 (2d Cir. 2000) 37.2, 37.7.2
Grand Jury Proceedings, In re, 532 F.2d 404 (5th Cir.), cert. denied, 429 U.S. 940 ..... 40.1, 40.5
Grand Jury Proceedings, In re, 87 F.3d 377 (9th Cir. 1996) 37.1.1.1
Grand Jury Proceedings, In re, No. M–11–189 (LAP), 2001 WL 1167497 (S.D.N.Y. 3 October 2001) 37.7
Grand Jury Subpoena dated Aug. 9, 2000, In re, 218 F. Supp. 2d 544 (S.D.N.Y. 2002) 40.1
Grand Jury Subpoena Duces Tecum, In re, 191 F.3d 173, 178 (2d Cir. 1999) 18.5.3
Grand Jury Subpoena Duces Tecum, In re, 406 F. Supp. 381 (S.D.N.Y. 1975) 37.1.3
Grand Jury Subpoena Duces Tecum, In re, 439 F.3d 740 (D.C. Cir. 2006) 35.3.1.2
Grand Jury Subpoena Duces Tecum, In re, 731 F.2d 1032 (2d Cir. 1984) 37.1.1.1
Grand Jury Subpoena Duces Tecum, In re, 738 F.2d 1367 (D.C. Cir. 1984) 37.5
Grand Jury Subpoena Duces Tecum, In re, 773 F.2d 204 (8th Cir. 1985) 37.1.1.1
Grand Jury Subpoena, In re, 223 F.3d 213 (3d Cir. 2000) 37.1.1.1
Grand Jury Subpoena, In re, 265 F. Supp. 2d 321 (S.D.N.Y. 2003) 37.7, 39.1.6, 39.3.2
Grand Jury Subpoena: Under Seal In re, 415 F.3d 333 (4th Cir. 2005) 18.4.4
Grand Jury Subpoenas, In re, 454 F.3d 511 (6th Cir. 2006) 37.6
Green v. Cosby, No. 3:14–cv–30211 (D. Mass. filed 10 December 2014) 39.3.1
Griffin v. Maryland, 19 A.3d 415 (Md. 2011) 39.2.1
Gruss v. Zwirn, 2013 WL 3481350, at *5–8 (S.D.N.Y. 10 July 2013) 24.3.1
Guggenheim Capital, LLC v. Birnbaum, 722 F.3d 444 (2d Cir. 2013) 35.2.2
Guiffre v. Maxwell, No. 15 Civ. 7433 (RWS), 2016 U.S. Dist. LEXIS 58204 (S.D.N.Y. 2 May 2016) 37.7
Guth v. Loft, Inc., 5 A.2d 503 (1939) 43.2.2
Guttman v. Huang, 823 A.2d 492 (Del. Ch. 2003) 43.3.1
Haines v. Liggett Grp, 975 F.2d 81 (3d Cir. 1992) 37.1.1
Halebian v. Berv, 644 F.3d 122, 127 n.4 (2d Cir. 2011) 35.3.2.2
Hamilton v. Carell, 243 F.3d 992 (6th Cir. 2001) 1.1.2
Hannaford Bros. Co. Customer Data Sec. Breach Litig., In re, 613 F. Supp. 2d 108, 119–20 (D. Me. 2009) 41.5.3
Hartford Fire Insurance Co v. California, 509 U.S. 764, 795–96 (1993) 29.7
Hatamian v. Advanced Micro Devices, Inc., Case No. 14-cv-00226-YGR (JSC), 2016 U.S. Dist. LEXIS 60551, at *4 (N.D. Cal. 6 May 2016) 8.5

© Law Business Research 2021

Haugh v. Schroder Inv. Management N. Am, Inc., No. 02 Civ. 7955 (DLC), 2003 U.S. Dist. Lexis 14586 (S.D.N.Y. 25 August 2003) 37.7, 39.1.6
Haugh v. Schroder Inv. Management N. Am, Inc., 02-7955, 2003 WL 21998674, at *3 (S.D.N.Y. 25 August 2003) 18.6
Haxhiaj v. Hackman, 528 F.3d 282, 292 (4th Cir. 2008) 18.3.2
Hechinger Inv. Co, In re, 285 B.R. 601 (D. Del. 2002) 37.2
Henry Schein Practice Sols., Inc., In re, FTC File No. 142-3161, No. C-4575 (F.T.C. 20 May 2016), 2016 WL 160609 ..... 41.5.3
Herbal Supplements Mktg. & Sales Practices Litig., In re, 2017 WL 2215025, at *6 (N.D. Ill. 19 May 2017) 24.5.4
Hermelin v. K–V Pharm. Co, 54 A.3d 1093 (Del. Ch. 2012) 14.6.2.2
Herrera. *See* Securities Exchange Commission v. Herrera
Hertzberg v. Veneman, 273 F. Supp. 2d 67 (D.D.C. 2003) 37.1.2
Hickman v. Taylor 329 U.S. 495 (1947) 8.5, 37.1.2
Highlander Holdings, Inc. v. Fellner, 2020 WL 3498174, at *12 (S.D. Cal. 29 June 2020) 35.2.2
Hill v. Cosby, No. 15–1658, 2016 U.S. Dist. LEXIS 7300 (W.D. Pa. 21 January 2016) 39.3.1
Hoiles v. Superior Court, 204 Cal. Rptr. 111 (Cal. Ct. App. 1984) 37.1.1.2
Hooker v. Klein, 573 F.2d 1360, 1369 (9th Cir. 1978) 18.3.5
HSBC Bank USA NA, 2016 WL 34760, at *1, *6 ..... 33.5.5
HSBC Holdings plc, In re, (10 December 2012) 24.4.1
Hsiung v. United States, No. 14-1121 (16 March 2015), cert. denied, 135 S. Ct. 2837 (15 June 2015) 29.7
Hudson v. United States, 522 U.S. 93 (1997) 1.2.2
Hughey v. United States, 495 U.S. 411 (1990) 31.2.6
Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc., 892 F.3d 612 (4th Cir. 2018) 41.5.3
IAP Worldwide Services Inc., NPA, FCPA claims, In re, (Department of Justice June 2015) 24.4.1, 24.5.4
ING Bank N.V, In re, (8 June 2012) 24.4.1
Initial Pub. Offering Sec. Litig., In re, 2004 WL 60290, at *2 (S.D.N.Y. 12 January 2004) ... 24.3.1
Intuniv Antitrust Litig., In re, 2020 WL 4274507, at *4 (D. Mass. 24 July 2020) 35.3.3.2
John Doe Corp., In re, 675 F.2d 482 (2d Cir. 1982) 6.4
Johnson v. Greater Se. Cmty. Hosp. Corp., 951 F.2d 1268 (D.C. Cir. 1991) 39.1.2
Jones v. Federated Fin. Reserve Corp., 144 F.3d 961 (6th Cir. 1998) 1.1.2
JP Morgan Securities In re, (Asia Pacific) (Department of Justice 17 November 2016) 24.4.1
JP Morgan Securities Inc. v. Vigilant Ins. Co, 126 A.D.3d 76 (N.Y. App. Div. 1st Department 2015) 24.5.4
Judson Atkinson Candies, Inc. v. Latini–Hohberger Dhimantec, Inc., 529 F.3d 371 (7th Cir. 2008) 37.2
Kaley v. United States, 571 U.S. 320, 328 (2014) 18.6
Kastigar v. United States, 406 U.S. 441 (1972) 18.4.2.1, 35.2.2
KBR, Inc., In the Matter of. *See* Securities and Exchange Commission v. KBR
KBR, Inc. *See also* Kellogg Brown & Root, Inc.
Keeper of the Records, In re, 348 F.3d 16 (1st Cir. 2003) 37.4
Kellher v. City of Reading, No. CIV.A.01-3386, 2002 WL 1067442, at *1 (E.D. Pa. 29 May 2002) 18.3.5
Kellogg Brown & Root, Inc., In re, 756 F.3d 754 (D.C. Cir. 2014) 6.4, 37.3.1
Khazin v. TD Ameritrade Holding Corp., 773 F.3d 488 (3d Cir. 2014) 20.2.3
Kimbrough v. United States, 552 U.S. 85 (2007) 31.2.1
Kiobel v. Royal Dutch Petroleum Co, 569 U.S. 108 (2013) 29.1, 29.3
Klein v. Harris, 667 F.2d 274 (2d Cir. 1981) 35.2.2

© Law Business Research 2021

Kokesh v. Securities Exchange Commission, 137 S. Ct. 1635 (2017) 24.5.1, 26.4
Kottler v. Deutsche Bank AG, 607 F. Supp. 2d 447 (S.D.N.Y. 2009) 24.5.4
Koumoulis v. Independent Financial Marketing Group Inc., 83 295 F.R.D. 28 (E.D.N.Y. 1 November 2013), aff'd in part, 29 F. Supp. 3d 142 (E.D.N.Y. 21 January 2014) 37.3.3
Lagos v. United States, 138 S. Ct. 1684, 1685-6 (2018) 10.2.3, 31.2.6
Laperriere v. Vesta Ins. Group, 526 F.3d 715, 723–25 (11th Cir. 2008) 43.4
Las Vegas Sands Corp., In re, (17 January 2017) 24.4.1
Lawrence v. Parker, No. 2019 WL 5704594, at *2 (W.D. Mich. 16 September 2019) 35.2.1
Lawson v. FMR LLC, 571 U.S. 429, 440 (2014) 20.1.1
Laydon v. Mizuho Bank Ltd, No. 12-cv-3419-GBD, 2015 WL 1515487 (S.D.N.Y. 31 March 2015) 29.5
Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (N.D Ohio 2013) 14.4.2, 40.3
Leasco Data Processing Equip. Corp. v. Maxwell, 468 F.2d 1326 (2d Cir. 1972) 29.2.1
Leegin Creative Leather Prods, Inc. v. PSKS, Inc., 551 US 877 (2007) 29.7
Legg Mason, Inc., In re, (4 June 2018) 24.4.1
Leocal v. Ashcroft, 543 U.S. 1, 12 n.8 (2004) 29.3
Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) 18.5.3, 40.3
LiButti v. United States, 107 F.3d 110, 113 (2d Cir. 1997) 35.2.2
Linde v. Arab Bank, PLC, 706 F.3d 92 (2d Cir. 2013) 40.5
Lipsky v. Commonwealth United Corp., 551 F.2d 887 (2d Cir. 1976) 24.5.4
Li Tao Hu, In re, ALJ Case No. 2017-SOX-00019, 2019 WL 5089597, at *5 (18 Sep. 2019) 20.2.3
Liu v. Securities and Exchange Commission No. 18–501, 2020 WL 3405845, (U.S. 22 June 2020) 26.4, 26.7.1
Liu v. Securities and Exchange Commission, 140 S. Ct. 1936 (2020) 24.5.1
Liu Meng–Lin v. Siemens AG, 763 F.3d 175 (2d Cir. 2014) 20.2.3
Livingston v. Wyeth Inc., 2006 WL 2129794 (M.D.N.C. 28 July 2006) 20.2.3
Loginovskaya v. Batratchenko, 764 F.3d 266 (2d Cir. 2014) 29.6
Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC, 797 F.3d 160, 179 n.11 (2d Cir. 2015) 35.4.1
Lotes Co., Ltd. v. Hon Hai Precision Indus. Co., 753 F.3d 395, 413–14 (2d Cir. 2014) 29.7
Louis Vuitton Malletier S.A. v. LY USA, Inc., 676 F.3d 83, 97 to 99 (2d Cir. 2012) 35.2, 35.2.1
Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 113 (2d Cir. 2006) 35.4.3
Luis v. United States, 136 S. Ct. 1083 (2016) 31.2.5.1
MacCartney v. O'Dell, 2018 WL 5023947, at *2 (S.D.N.Y. 2018) 35.4.3
Mackin, In re, 668 F.2d 122, 127-28 (2d Cir. 1981) 18.3.5
Mahony v. KeySpan Corp., No. 04 CV 554 SJ, 2007 WL 805813 (E.D.N.Y. 12 March 2007) 20.2.3
Manrique, In re, No. 3:19-mj-71055-MAG (N.D. Cal. 19 March 2020) 18.2.1
Martin Marietta Corp. v. Pollard, In re, 856 F.2d 619 (4th Cir. 1988) 37.5
Martinez v. Illinois, 134 S. Ct. 2070, 2074 ..... 1.2.2
Martinez v. City of New York, 2018 WL 582321, at *1 (E.D.N.Y. 26 January 2018) 35.4.3
Marx v. Akers, 88 N.Y.2d 189 (N.Y. 1996) 35.3.2.2
Menaldi v. Och-Ziff Capital Mgmt. Grp. LLC, 277 F. Supp. 3d 500, 509 (S.D.N.Y. 2017) .. 24.5.4
Merrill Lynch & Co v. Allegheny Energy Inc., 229 F.R.D. 441 (S.D.N.Y. 2004) 37.7.1
Mesirov v. Enbridge Energy Co., Inc., No. CV 11314-VCS, 2018 WL 4182204, at *8 (Del. Ch. 29 August 2018) 35.3.2.2
Meyer v. Fleming, 327 U.S. 161, 167 (1946) 35.3.2.2
Microfinancial, Inc. v. Premier Holidays Int'l, Inc., 385 F.3d 72, 78 (1st Cir. 2004) 35.2.1
Minn-Chem, Inc. v. Agrium, Inc., 683 F.3d 845, 855 (7th Cir. 2012) 29.7
Miranda v. Arizona, 384 U.S. 436 (1966) 14.3
Mirchandani v. United States, 836 F.2d 1223, 1226 (9th Cir. 1988) 18.3.5

© Law Business Research 2021

Morgan Art Found. Ltd v. McKenzie, 2020 WL 3578251, at * (S.D.N.Y. 1 July 2020).....24.3.1
Morris v. Spectra Energy Partners (DE) GP, LP, Civil Action No. 12110–VCG, 2018 WL 2095241 (Del. Ch. 7 May 2018).....37.1.1.2
Morrison v. National Australia Bank Ltd 561 US 247 (2010).....29.1, 29.2, 29.2.1, 29.2.2, 29.3, 29.4, 29.5, 29.6, 29.7, 29.8
Morrison v. National Australia Bank, 67 N.Y.U. Ann. Surv. Am. L. 137, 169–70 (2011).....29.3
Morse/Diesel, Inc. v. Fidelity & Deposit Co of Maryland, 122 F.R.D. 447 (S.D.N.Y. 1988) 35.5.3
Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816 (7th Cir. 2015) 29.7
Motorola Credit Corp. v. Uzan, 293 F.R.D. 595 (S.D.N.Y. 2013).....40.5
Motorola, Inc. v. Lemko Corp., No. 08 C 5427, 2010 WL 2179170 (N.D. Ill. 1 June 2010) .37.1.1
Mott v. Anheuser–Busch, Inc., 910 F. Supp. 868 (N.D.N.Y. 1995) 35.3.3.3
MP Corp. v. Redbridge Bedford, LLC, 128 N.E.3d 128, 134 (N.Y. 2019) 35.3.3.1
Muick v. Glenayre Elecs, 280 F.3d 741 (7 Cir. 2002) 40.3
Murphy v. Gorman, 271 F.R.D. 296, 311-313 (D.N.M. 2010) 37.1.1.2
Murray v. UBS Sec, LLC, 2014 WL 285093 (S.D.N.Y. 27 January 2014).....20.2.3
Mut. Funds Inv. Litig., In re, 566 F.3d 111, 129–30 (4th Cir. 2009).....43.5
Myun-Uk Choi v. Tower Research Capital LLC, 890 F.3d 60, 66 (2d Cir. 2018)..... 29.2.2, 29.6
Myspace LLC, In the Matter of, Docket No. C-4369 (F.T.C. 11 September 2012) 41.5.3
N.L.R.B. v. J. Weingarten, Inc., 420 U.S. 251 (1975).....14.3
Nam v. U.S. Express, Inc., 2012 WL 12840094, at *3 (E.D.Tenn. 15 May 2012) 8.5
NAMA Holdings, LLC v. Greenberg Traurig, LLP, 18 N.Y.S.3d 1 (N.Y. App. Div. 2015) 37.1.1.2
Narayanan v. Southern Global Holdings Inc., 285 F. Supp. 3d 604 (W.D.N.Y. 2018).....37.7
Nat'l City Golf Fin. v. Higher Ground Country Club Management Co, LLC, 641 F. Supp. 2d 196 (S.D.N.Y. 2009).....20.2.3
Nat'l Union Fire Ins. Co of Pittsburgh, PA v. AARPO, Inc., No. 97–CV–1438, 1998 U.S. Dist. LEXIS 21342 (S.D.N.Y. 24 November 1998).....2.3.3
Natural Gas Commodity Litigation, In re, 2005 WL 1457666 No. 03 Civ. 6186 (VM) (AJP), 2005 U.S. Dist. Lexis 11950 (S.D.N.Y. 21 June 2005) 24.3.1, 37.5
Navient Sols., LLC v. Law Offices of Jeffrey Lohman, 19-cv-461, 2020 WL 1917837, *6 (E.D. Va. 20 April 2020) 37.1.1.1
Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976).....39.1.2
New Jersey Bell Tel. Co & Local 827, Int'l Bhd. of Elec. Workers, Afl–Cio, 308 NLRB 277, 279–80 (1992).....14.3
Nielsen v. AECOM Tech. Corp., 762 F.3d 214 (2d Cir. 2014.....20.2.3
No–Action Letter, Dougherty & Co, 2003 WL 22204509 (Securities Exchange Commission 3 July 2003) 24.5.3
Norris v. Government of the United States [2008] 1 AC 920 .....32.3.1
Ntakirutimana v. Reno, 184 F.3d 419, 423 (5th Cir. 1999).....18.3.5
NXIVM Corp. v. O'Hara, 241 F.R.D. 109 (N.D.N.Y. 2007) 8.4, 37.7
O'Connor v. Ortega, 480 US 709 (1987).....40.3
O'Mahony v. Accenture Ltd, 537 F. Supp. 2d 506 (S.D.N.Y. 2008).....20.2.3
Oen Yin-Choy v. Robinson, 858 F.2d 1400, 1407 (9th Cir. 1988) 18.3.3
OSG Sec. Litig., In re, 12 F. Supp. 3d 619, 621 (S.D.N.Y. 2014).....24.5.4
Ott v. Fred Alger Mgmt, Inc., 2012 WL 4767200 (S.D.N.Y. 27 September 2012) ... 20.1.1, 20.2.3
Pacific Fertility Center Litigation, Case No. 18-cv-01586-JSC, 2020 U.S. Dist. LEXIS 71127, at *8-9 (N.D. Cal. 22 April 2020) 2.3.5
Pacific Pictures Corp. v. United States Dist. Court, 679 F.3d 1121, No. 11–71844, 2012 U.S. App. LEXIS 7643 (9th Cir. 17 April 2012) 2.3.3, 24.3.1, 37.5
Paradigm Capital Management, Inc., In re, S.E.C. File No. 3–15930 (2014)..... 20.2.3, 20.2.4

© Law Business Research 2021

Parkcentral Global Hub Ltd v. Porsche Auto Holdings SE, 763 F.3d 198 (2d Cir. 2014) 29.2.2, 29.6
Pasquantino v. United States, 544 U.S. 349 (2005) 29.5
Patel v. Facebook, 18-15982 (9th Cir. 8 August 2019) 40.3
Pearson v. Rock, No. 12–CV–3505, 2015 WL 4509610 (E.D.N.Y. 24 July 2015) 39.1.3
People v. Harris, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012) 39.2.1
People of the State of Illinois v. Uber Technologies Inc., No. 2018-CH-000304, final judgment and consent decree, September 2018 ..... 41.1.3
Peralta v. Cendant Corp., 190 F.R.D. 38 (D. Conn. 1999) 37.3.2
Permian Corp. v. United States, 665 F.2d 1214 (D.C. Cir. 1981) 37.5
Petrobas Sec., In re, 862 F.3d 250, 262 (2d Cir. 2017) 29.2.2
Pittsburgh History & Landmarks Foundation v. Ziegler, J-26A-2018 (Pa. Jan. 23, 2019) 6.3
Pittsburgh History & Landmarks Foundation v. Zeigler, 200 A.3d 58 (Pa. 2019) 37.1.1.2
Platinum & Palladium Commodities Litigation In re, 828 F. Supp. 2d 588 (S.D.N.Y. 13 September 2011) 24.5.4
Polk v. KV Pharm. Co., 2011 WL 6257466, at *6 (E.D. Mo. 15 December 2011) 24.5.4
Premera Blue Cross Customer Data Security Breach Litigation, In re, 296 F. Supp. 3d 1230 (D. Or. 2017) 37.7
Press–Enterprise Co v. Superior Court of California, 478 U.S. 1 (1986), 106 S. Ct. 2735 ..... 39.1.1
Press–Enterprise Co v. Superior Court of California, Riverside Cty, 464 U.S. 501 (1984) 39.1.1
Prime Int'l Trading, Ltd. v. BP P.L.C., 937 F.3d 94, 104-07 (2d Cir. 2019) 29.2.2, 29.6
Puerto Rico v. Sanchez Valle, 136 S. Ct. 1863 (2016) 1.2.2
Quinn v. Robinson, 783 F.2d 776, 817 n.41 (9th Cir. 1986) 18.3.3
Qwest Commc'ns Int'l, Inc., In re, 450 F.3d 1179 (10th Cir. 2006) (Securities Exchange Commission and Department of Justice Investigations) 24.3.1, 37.1.2
Rene v. G.F. Fishers, Inc., 817 F. Supp.2d 1090 (S.D. Ind. 2011) 40.3
Republic of Turkey v. Christie's, Inc., 326 F.R.D. 394, 399 (S.D.N.Y. 2018) 24.3.1
Requested Extradition of Kirby, In re, 106 F.3d 855, 867 (9th Cir. 1996) 18.3.2
Restasis Antitrust Litigation, In re, 352 F. Supp. 3d. 207, 214-215 (E.D.N.Y. 2019) 37.7
Richard Roe Inc. v. Richard Roe Inc., In re, 68 F.3d 38 (2d Cir. 1995) 37.1.1
Richman v. Goldman Sachs Grp, Inc., 868 F. Supp. 2d 261 (S.D.N.Y. 2012) 24.3.1
Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) 39.1.1
Riddle v. First Tenn. Bank, 497 F. App'x. 588 (6th Cir. 2012) 20.1.1
Ridenour v. Kaiser–Hill Co, 397 F.3d 925 (10th Cir. 2005) 20.4.1
Rinaldi v. United States, 434 U.S. 22 (1977) 31.1.1
Rio Tinto PLC v. Vale S.A., 2014 WL 7191250, at *1 (S.D.N.Y. 17 December 2014) 35.3.3.2
RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016) 29.1, 29.3, 29.4, 29.5
Roberts v. Accenture, LLP, 707 F.3d 1011, 1015 (8th Cir. 2013) 20.4.1
Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34 (Ill. 2019) 40.3
Rough Rice Commodity Litig., In re, 2012 WL 473091, at *5 (N.D. Ill. 9 February 2012) 24.5.4
Rowe v. Guardian Auto. Prods, 2005 WL 3299766 (N.D. Ohio 6 December 2005) 40.3
Rubenstein v. Cosmos Holdings Inc., 2020 WL 3893347 *11 (S.D.N.Y. 10 July 2020) 29.2.2
Ruhe v. Masimo Corp., 2011 WL 4442790 (C.D. Cal. 16 September 2011) 20.2.3
Ryan, In re, 360 F. Supp. 270, 275 (E.D.N.Y. 1973), aff'd, 478 F.2d 1397 (2d Cir. 1973) 18.3.4
Ryniewicz v. Clarivate Analytics, 803 F. App'x 858, 867 (6th Cir. 2020) 35.3.3.4
Safford v. St. Tammany Parish Fire Prot. Dist. No. 1, 2003 U.S. Dist. LEXIS 6513 (E.D. La. 11 April 2003) 35.4.1
Salomon Forex Inc. v. Tauber, 795 F. Supp. 768, 771 (E.D. Va. 1992) 29.6
Salzberg v. Sciabacucchi, 227 A.3d 102 (Del. 2020) 35.3.2.2
Shapiro v. Ferrandina, 478 F.2d 894, 901 (2d Cir. 1973) 18.3.4

© Law Business Research 2021

Schoenbaum v. Firstbrook, 405 F.2d 200 (2d Cir. 1968)..... 29.2.1, 29.7
Scott v. Beth Israel Med. Ctr, Inc., 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007) 40.3
Scott v. Chipotle Mexican Grill, 94 F. Supp. 3d 585 (S.D.N.Y. 2015).....39.1.6
Sealed Case, In re, 754 F.2d 395 (D.C. Cir. 1985).....37.1.1.1
Sealed Case, In re, 754 F.2d 402.....37.1.1.1
Sealed Case, In re: No. 19-5068 (D.C. Cir. 6 August 2019).....29.1
Sealed Case, In re; 932 F.3d 915 (D.C. Cir. 2019).....29.11
Sealed Party v. Sealed Party, No. 04–2229, 2006 U.S. Dist. LEXIS 28392 (S.D. Tex. 4 May 2006).....39.1.1
Search Warrant, In re, 942 F.3d.....37.6
Search Warrant Issued 13 June 2019, In re, 942 F.3d 159, 183 (4th Cir. 2019).....37.6
Searcy v. Philips Elecs. N. Am. Corp., 117 F.3d 154 (5th Cir. 1997).....20.4.1
Sears Holdings Mgmt. Corp., In re, Docket No. C-4264, para. 4 (F.T.C. 9 September 2009)...41.5.3
Securities and Exchange Commission v. Ahmed, 308 F. Supp. 3d 628, 660–64 (D. Conn. 2018).....29.2.2
Securities and Exchange Commission v. Aronson, 665 F. App'x 78 (2d Cir. 2016).....24.4.1
Securities and Exchange Commission v. Berger, 322 F.3d 187 (2d Cir. 2003) 29.2.1
Securities and Exchange Commission v. Cavanagh, 2004 WL 1594818 (S.D.N.Y. 16 July 2004), aff'd, 445 F.3d 105 (2d Cir. 2006).....26.4
Securities and Exchange Commission v. Chicago Convention Center, LLC, 961 F. Supp. 2d 905 (N.D. Ill. 2013) 29.2.2
Securities and Exchange Commission v. Citigroup Global Markets, Inc., 752 F.3d 285 (2d Cir. 2014) 24.4.1
Securities and Exchange Commission v. Contorinis, 743 F.3d 296 (2d Cir. 2014).....26.4
Securities and Exchange Commission v. CR Intrinsic Investors, LLC, 939 F. Supp. 2d 431 (S.D.N.Y. 2013).....24.4.1
Securities and Exchange Commission v. Desai, 672 F. App'x 201, 205 n.5 (3d Cir. 1 December 2016).....35.2.1
Securities and Exchange Commission v. DiBella, 2008 WL 6965807 (D. Conn. 18 July 2008)26.4
Securities and Exchange Commission v. Ficeto, 839 F. Supp. 2d 1101, 1108 (C.D. Cal. 2011) 29.2.2
Securities and Exchange Commission v. First Jersey Sec, Inc., 101 F.3d 1450 (2d Cir. 1996) ...26.4
Securities and Exchange Commission v. GMC Holding Corp., 2009 WL 506872 (M.D. Fla. 27 February 2009) 26.4
Securities and Exchange Commission v. Herrera, 324 F.R.D. 258 (S.D. Fl. 2017) 37.5
Securities and Exchange Commission v. Huffman, 996 F.2d 800 (5th Cir. 1993).....26.4
Securities and Exchange Commission v. KBR, Release No. 34–74619 (1 April 2015). 2.4.2, 20.2.2
Securities and Exchange Commission v. KBR, No. 3–16466 (1 April 2015) 20.2.4
Securities and Exchange Commission v. Montano, 2020 WL 5534653 *7 (M.D. Fla. 24 July 2020) 29.2.2
Securities and Exchange Commission v. Mulvaney, 2012 WL 12930425 (E.D. Wis. 20 November 2012).....24.4.1
Securities and Exchange Commission v. Nature's Sunshine Prods., Inc., Civ. No. 2:09CV0672, Compl. (D. Utah 31 July 2009) 43.4
Securities and Exchange Commission v. One or More Unknown Traders in the Securities of Onyx Pharmaceuticals, Inc., 296 F.R.D. 241 (S.D.N.Y. 2013) 18.6
Securities and Exchange Commission v. Page Airways, Inc. 33.2.1
Securities and Exchange Commission v. Rashid, 17-cv-8223, 2018 WL 6573451 (PKC) (S.D.N.Y. 13 December 2018)..... 16.2.3, 37.1.3
Securities and Exchange Commission v. Roberts, 254 F.R.D. 371 (N.D. Cal. 2008) 2.3.3

© Law Business Research 2021

Securities and Exchange Commission v. Savino, 2006 WL 375074 (S.D.N.Y. 16 February 2006) 26.4
Securities and Exchange Commission v. Schroeder, No. C07–03798 JW, 2009 U.S. Dist. LEXIS 39378 (N.D. Cal. 27 April 2009) 2.3.3
Securities and Exchange Commission v. Scoville, 913 F.3d 1204, 1218 (10th Cir.), cert. denied, 18–1566 (4 November 2019) 29.2.2
Securities and Exchange Commission v. Straub, 921 F. Supp. 2d 244 (S.D.N.Y. 2013) 29.8
Securities and Exchange Commission v. Teva Pharmaceutical Industries, Ltd, 1:16–cv–25298 (S.D. Fla. 22 December 2016) 24.6.1
Securities and Exchange Commission v. Thrasher, 1996 WL 94533 (S.D.N.Y. 27 February 1996) 24.3.1
Securities and Exchange Commission v. Unifund SAL, 910 F.2d 1028 (2d Cir. 1990) 18.6
Securities and Exchange Commission v. United Energy Partners, Inc., 2003 WL 223392 (N.D. Tex. 28 January 2003), aff'd, 88 F. App'x 744 (5th Cir. 2004) 26.4
Securities and Exchange Commission v. VimpelCom Ltd (now known as VEON) 24.6.2
Securities and Exchange Commission v. Yun, 148 F. Supp. 2d 1287 (M.D. Fla. 2001) 26.4
Sharkey v. JP Morgan Chase & Co, No. 10 Civ. 3824, 2011 WL 135026 (S.D.N.Y. 14 January 2011) 20.1.1
Shaev Profit Sharing Account v. Armstrong, C.A. No. 1449-N, 2006 Del. Ch. LEXIS 33, at *16 (Del. Ch. 13 February 2006) 43.6
Shearson/Am. Express Inc. v. McMahon, 482 U.S. 220 (1987) 20.2.3
Sheppard v. Maxwell, 384 U.S. 333 (1966) 39.1.2, 39.3.1
Sims v. Lakeside School, No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. 20 September 2007) 18.5.3
Skilling v. United States, 561 U.S. 358, 369 n.1 (2010) 29.5
Small v. Nobel Biocare USA, LLC, 808 F. Supp. 2d 584 (S.D.N.Y. 2011) 24.3.1
Smith v. Van Gorkom, 488 A.2d 858, 881 (Del. 1985) 43.2.1
Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) 18.5.3
Société Nationale Industrielle Aérospatiale v. United States Dist. Court for S. Dist, 482 U.S 522 (1987) 40.5
Soe v. Sex Offender Registry Bd., 995 N.E.2d 73, 80 (Mass. 2013) 35.2.1
Sonterra Capital Master Fund Ltd v. Credit Suisse Grp. AG, 277 F. Supp. 3d 521 (S.D.N.Y. 2017) 29.5, 29.7
Southern Union Co v. United States, 132 S. Ct. 2344 (2012) 26.2.1
Steinhardt Partners, L.P, In re, 9 F.3d 230 (2d Cir. 1993) 24.3.1, 37.5
Stewart v. Doral Fin. Corp., 997 F. Supp. 2d 129 (S.D.N.Y. 2014) 20.1.1
Stockman v. Oakcrest Dental Center P.C, 480 F.3d 791 (6th Cir. 2007) 35.5.2
Stone v. Ritter, 911 A.2d 362, 369 (Del. 2006) 43.2.2, 43.3.1
Stoyas v. Toshiba Corp., 896 F.3d 933, 945–47 (9th Cir. 2018) 29.2.2
Strauss v. Credit Lyonnais, S.A, No. 06–CV–702, 2011 WL 4736359 (E.D.N.Y. 6 October 2011) 39.1.2
Subpoena Duces Tecum, In re, 439 F.3d 740, 753 to 754 (D.C. Cir. 2006) 35.3.1.2
Sullivan v. Barclays PLC, No. 13-cv-2811-PKC, 2017 WL 685570, at *29 (S.D.N.Y. 21 February 2017) 29.6, 29.7
Superintendent of Her Majesty's Foxhill Prison & United States v. Kozeny, Privy Council Appeal No. 0073, s.53 (Judicial Comm. of the Privy Council 28 March 2012) (Bah) 18.3.4
Swidler & Berlin v. United States, 524 U.S. 399 (1998) 8.4, 18.5.1, 37.1.1, 37.1.1.1
Swift Spindrift, Ltd v. Alvada Ins. Inc., No. 09 Civ. 9342 (AJN)(FM), 2013 WL 3815970 (S.D.N.Y. 24 July 2013) 37.4

© Law Business Research 2021

Sylvester v. Parexel Int'l LLC, 2011 WL 2165854, ARB No. 07–123, ALJ Nos. 2007–SOX–039, –042 (ARB 23 May 2011) 20.1.1
Synthes Spine v. Walden, 232 F.R.D. 460 (E.D. Pa. 2005) 37.8
Target Corp. Customer Data Sec. Breach Litig., In re, 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014) 41.5.3
TD Bank N.A., In the Matter of, (23 September 2013) 24.5.4, 24.6.1
Teleglobe Commc'ns Corp., In re, 493 F.3d 345 (3d Cir. 2007) 37.4
Telia case. *See* United States v. Telia Co AB
Tellez v. OTG Interactive, LLC, 2019 WL 2343202, at *4 (S.D.N.Y. 3 June 2019) 20.1.1
Tenaris S.A. In re, (Department of Justice 17 May 2011) 24.4.1
Thompson v. United States, 444 U.S. 248 (1980) 1.2.2
Thygeson v. U.S. Bancorp, 2004 U.S. Dist LEXIS 18863 (D. Or. 15 September 2004) 40.3
Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012) 39.2.1
Tiffany (NJ) LL v. Qi Andrew, et al, 276 F.R.D. 143 (S.D.N.Y. 2011) 40.5
Tiffany (NJ) LLC v. Forbse, 2012 WL 1918866 (S.D.N.Y. 23 May 2012) 40.5
Tobia v. United Grp. of Cos, Inc., 2016 WL 5417824 (N.D.N.Y. 22 September 2016) 24.5.4
Tokar v. United States Department of Justice, No. 16–2410, 2018 WL 1542320 (D.D.C. 29 March 2018) 33.4
Tribune Co v. Purcigliotti, 1996 WL 337277 (S.D.N.Y. 19 June 1996) 24.3.1
Tri-Star Pictures, Inc. Litig., In re, 634 A.2d 319, 333 (Del. 1993) 43.3.1
Twelve Grand Jury Subpoenas, In re, 908 F.3d 525, 528 (9th Cir. 2018) 35.2.2
Ulrich v. Moody's Corp., 721 Fed.Appx. 17, 19 (2d Cir. 2018) 20.2.3
United States Dept. of Educ. v. National Collegiate Athletic Ass'n, 481 F.3d 936 (7th Cir. 2007) 37.7
United States ex rel. Doe v. Heart Solutions PC et al., 923 F.3d 308, 314-15 (3d Cir. 2019) 37.4.1
United States ex rel. Downy v. Corning, Inc., 118 F. Supp. 2d 1160 (D.N.M. 2000) 20.4.1
United States ex rel. Hunt v. Merck–Medco Managed Care, LLC, 340 F. Supp. 2d 554 (E.D. Pa. 2004) 37.3.2
United States ex rel. Jamison v. McKesson Corp., 649 F.3d 322 (5th Cir. 2011) 20.4.1
United States ex rel. Karvelas v. Melrose–Wakefield Hosp, 360 F.3d 220 (1st Cir. 2004) 20.4.1
United States ex rel. Killingsworth v. Northrop Corp., 25 F.3d 715 (9th Cir. 1994) 20.4.1
United States ex rel. Mikes v. Straus, 78 F. Supp. 2d 223 (S.D.N.Y. 1999) 20.4.1
United States ex rel. Pilon v. Martin Marietta Corp., 60 F.3d 995 (2d Cir. 1995) 20.4.2
United States ex rel. Saroop v. Garcia, 109 F.3d 165, 168 (3d Cir. 1997) 18.3.3
United States ex rel. Sequoia Orange Co v. Baird–Neece Packing Corp., 151 F.3d 1139 (9th Cir. 1998) 20.4.1
United States ex rel. Springfield Terminal Ry. Co v. Quinn, 14 F.3d 645 (D.C. Cir. 1994) 20.4, 20.4.1
United States ex rel. Touhy v. Ragen, 340 U.S. 462 (1951) 35.3.1.2
United States ex rel. Wenzel v. Pfizer, Inc., 881 F. Supp. 2d 217 (D. Mass. 2012) 20.4.2
United States ex rel. Williams v. Bell Helicopter Textron Inc., 417 F.3d 450 (5th Cir. 2005) 20.4.1
United States v. $1,071,251.44 of Funds Associated with Mingzheng Int'l Trading Ltd., 324 F. Supp. 3d 38, 43, 52 (D.D.C. 2018) 29.9
United States v. Abu Khatallah, 151 F. Supp. 3d 116, 124–26 (D.D.C. 2015) 29.3
United States v. Ackert, 169 F.3d 136 ..... 37.7
United States v. Adlman, 68 F.3d 1495 (2d Cir. 1995) 37.7
United States v. Ahmad, 101 F.3d 386 (5th Cir. 1996) 1.1.2
United States v. Airbus SE, Case No.: 1:20-cr-00021, Convention Judiciaire Intérêt Public between the Parquet National Financier and Airbus SE [2020] (PNF-16 159 000 839) 12.7
United States v. Aiyer, 433 F. Supp. 3d 468, 477 (S.D.N.Y. 2020) 39.2.2

© Law Business Research 2021

United States v. All Assets Held at Bank Julius, Baer & Co., Ltd., 315 F. Supp. 3d 90 (D.D.C. 2018) 29.3, 29.9, 29.10
United States v. All Assets Held at Bank Julius, Baer & Co., Ltd., 251 F. Supp. 3d 82, 103 (D.D.C. 27 April 2017) 29.3, 29.5, 29.9, 29.10
United States v. All Assets of Statewide Auto Parts, Inc., 971 F.2d 896, 905 (2d Cir. 1992) 35.2.2
United States v. Allen, 864 F.3d 63 (2d Cir. 2017) 12.4, 18.4.3.1
United States v. Allen, No. 16-898 (2d Cir. 2017) 3.5.2.1, 11.5.1
United States v. Almeida, 341 F.3d 1318 (11th Cir. 2003) 37.1.3
United States v. Alston, 609 F.2d 531, 536 (D.C. Cir. 1979) 29.5
United States v. Aluminum Co. of Am., 148 F.2d 416, 443–44 (2d Cir. 1945) 29.7
United States v. Amirnazmi, 645 F.3d 564, 579 (3d Cir. 2011) 29.9
United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002) 40.3
United States v. Apple Inc., 787 F.3d 131 (2d Cir. 2015) 33.2.1, 33.6
United States v. Apple Inc., 992 F. Supp. 2d 263 (S.D.N.Y. 2014) 33.6
United States v. Aramony, 88 F.3d 1369, 1392 (4th Cir. 1996) 18.4.4
United States v. Armstrong, 517 U.S. 456 (1996) 31.1.1
United States v. Assange, No. 1:18-cr-111 (E.D. Va. 6 March 2018) 18.3
United States v. Austin, 416 F.3d 1016, 1021 (9th Cir. 2005) 18.4.4
United States v. Automated Med. Labs, 770 F. 2d 399 (4th Cir. 1985) 1.1.2
United States v. Bank of New England, N.A, 821 F.2d 844 (1st Cir. 1987) 1.1.2
United States v. Barile, 2007 WL 3534261, at *2 (N.D.N.Y. 13 November 2007) 35.2.2
United States v. Barrow, 400 F. 3d 109, 113 to 119 (2d Cir. 2005) 16.5
United States v. Batchelder, 442 U.S. 114 (1979) 31.1.1
United States v. Bay State Ambulance, 874 F.2d 20 (1st Cir. 1989) 37.1.3
United States v. Blanco, 861 F.2d 773, 780 (2d Cir. 1988), cert. denied, 489 US 1019 (1989) 18.3.2
United States v. Blanton, 719 F.2d 815 (6th Cir. 1983) 39.1.3
United States v. Blumberg, 2017 U.S. Dist. LEXIS 47298 (D.N.J. 27 March 2017) 37.2
United States v. Booker, 543 U.S. 220, 125 S.Ct. 738, 160 L.Ed.2d 621 (2005) 26.2.2, 31.2.1
United States v. Boustani, No. 18-cr-681-WFK (E.D.N.Y. 22 July 2019), ECF No. 113 ..... 29.2.2
United States v. Boustani, No. 18-cr-681-WFK (E.D.N.Y. 21 June 2019), ECF No. 98 ..... 29.2.2
United States v. Boustani, No. 18-cr-681-WFK (E.D.N.Y. 13 September 2019), ECF No. 166 29.2.2
United States v. Boustani, No. 18-cr-681-WFK (E.D.N.Y. 3 October 2019), ECF No. 231 29.2.2
United States v. Bowman, 260 U.S. 94 (1922) 29.3
United States v. Butler, 543 F. App'x 95, 97 (2d Cir. 2013) 18.6
United States v. Cacace, 321 F. Supp. 2d 532 (E.D.N.Y. 2004) 39.1.3
United States v. Campa, 459 F.3d 1121 (11th Cir. 2006) 39.1.3
United States v. Coffman, 574 F. App'x 541 (6th Cir. 2014) 29.5
United States v. Connolly, No. 16 CR. 0370 (CM), 2019 WL 2120523, at *10 (S.D.N.Y. 2 May 2019) 10.2.6, 14.2, 18.4.2.2, 18.5.3, 37.3.1
United States v. Davis, 767 F.2d 1025 (2d Cir. 1985) 40.5
United States v. Driver, 692 F. App'x 448, 449 (9th Cir. 2017) 29.5
United States v. Duperval, 777 F.3d 1324 (11th Cir. 2015), cert. denied, 136 S. Ct. 859, L. Ed. 2d 757 (2016) 29.10
United States v. Dzhokhar A. Tsarnaev, No. 16-6001, 2020 WL 4381578 (1st Cir. 31 July 2020) 39.1.3
United States v. Epstein, 155 F. Supp. 2d 323, 326 (E.D. Pa. 2001) 18.2.1
United States v. Etkin, 2008 U.S. Dist. LEXIS 12834 (S.D.N.Y. 20 February 2008) 40.3
United States v. Facebook, Inc., No. 19-cv-02184 (D.D.C. 24 July 2019) 33.3
United States v. FedEx Corp., 2016 U.S. Dist LEXIS 52438 (N.D. Cal. 18 April 2016) 1.1.2

© Law Business Research 2021

United States v. First City Nat'l City Bank 396 F.2d 897 (2d Cir. 1968) 40.1, 40.5
United States v. Firtash, --- F. Supp. 3d ----, No. 13-cr-515, 2019 WL 2568569 (N.D. Ill. 21 June 2019) 29.8, 29.10
United States v. Fokker Services BV, 818 F.3d 733 (D.C. Cir. 2016), vacating 79 F. Supp. 3d 160 (D.D.C. 2015) 24.4.1, 33.4, 33.5.5
United States v. Gall, 552 U.S. 38 ..... 31.2.2
United States v. Garlick, 240 F.3d 789, 792 (9th Cir. 2001) 29.5
United States v. Gasperini, No. 16–CR–441 (NGG), 2017 WL 2399693 (E.D.N.Y. 1 June 2017) 29.5
United States v. Gasperini, 729 F. App'x 112, 113–14 (2d Cir. 2018) 29.4
United States v. Georgiou, 777 F.3d 125 (3d Cir. 2015) 29.2.2, 29.5
United States v. Gerena, 869 F.2d 82 (2d Cir. 1989) 39.1.1
United States v. Goldfarb, 2012 WL 3860756 (N.D. Cal. 5 September 2012) 24.5.4
United States v. Gorski 807 F.3d 451 (1st Cir. 2015) 37.1.1.1
United States v. Grace, 439 F. Supp.2d 1125 (D. Mont. 2006) 37.1.1.1
United States v. Graf, 610 F.3d 1148 (9th Cir.2010) 14.8, 37.2
United States v. Hatfield, 2009 WL 3806300 (E.D.N.Y. 2009) 16.2.3
United States v. Hawit, No. 15-cr-252-PKC, 2017 WL 663542, at *9–10 (E.D.N.Y. 17 February 2017) 29.4
United States v. Hayes 99 F. Supp. 3d 409 (S.D.N.Y.), aff'd on other grounds, 118 F. Supp. 3d 620 (S.D.N.Y. 2015), appeal dismissed (15 March 2016) 29.5
United States v. Henke, 222 F.3d 633 (9th Cir. 2000) 37.1.3
United States v. Hopkins, 53 F.3d 533 (2d Cir. 1995) 1.1.2
United States v. Horvath, 731 F.2d 557 (8th Cir. 1984) 37.1.1.1
United States v. Hoskins, 902 F.3d 69, 96 (2d Cir. 2018) 29.1, 29.8
United States v. Hoskins (D. Conn. Nov. 6, 2019) Trial Tr. 1246–47 ..... 29.8
United States v. Hoskins (D. Conn. Nov. 8, 2019) ECF No. 583 Jury Verdict 29.8
United States v. Hoskins F. Supp 3d 2020 WL 914302 *7 (D. Conn. 26 February 2020) 29.8
United States v. HSBC Bank USA NA, No. 12 CR 763 (JG), 2016 WL 347670 (E.D.N.Y. 28 January 2016), motion to certify appeal denied, No. 12–0763, 2016 WL 2593925 (EDNY 4 May 2016). 33.5.5
United States v. HSBC Bank USA, N.A, 2013 WL 3306161 (E.D.N.Y. 1 July 2013) 24.4.1
United States v. HSBC Bank USA, NA and HSBC Holdings Plc, 863 F, 3d 125 (2d Cir. 2017) 24.4.1, 33.5.5
United States v. Hubbell, 530 U.S. 27 (2000) 2.4.1
United States v. Hui Hsiung, 778 F.3d 738 (9th Cir. 2015) 29.7
United States v. Hussain, 972 F.3d 1138,1145 (9th Cir. 2020) 29.5
United States v. Int'l Bhd. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am, AFL–CIO, 119 F.3d 210 (2d Cir. 1997). 37.2
United States v. Jefferson, 674 F.3d 33, 336 (4th Cir. 2012) 29.5
United States v. JGC Corp., No. 11 CR 260, 2011 WL 1315939 (S.D. Tex. 6 April 2011) 29.8
United States v. Kordel, 397 U.S. 1, 7 (1970) 35.2.2
United States v. Kovel, 296 F.2d 918 (2d Cir. 1961) 2.3.5, 37.7, 39.1.6
United States v. Kozeny, 493 F. Supp. 2d 693, 706 (S.D.N.Y. 2007), aff'd, 541 F.3d 166 (2d Cir. 2008) 29.10
United States v. Lanza, 260 U.S. 377 (1922) 1.2.2
United States v. LaSalle Nat'l Bank, 437 U.S. 298, 313 (1978) 11.3
United States v. Laurins, 857 F.2d 529 (9th Cir. 1988) 37.1.1.1
United States v. LeCroy, 348 F. Supp. 2d 375, 387 (E.D. Pa. 2004), (10 January 2005) 16.2.3
United States v. Leija-Sanchez, 820 F.3d 899, 901 (7th Cir. 2016) 29.3

© Law Business Research 2021

United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004) 39.2.1
United States v. Lloyds TSB Bank PLC, 639 F. Supp. 2d 314, 324 n.4 (S.D.N.Y. 2009) 29.10
United States v. Lomeli, 596 F.3d 496, 501 (8th Cir. 2010) 18.3.4
United States v. Lopesierra-Gutierrez, 708 F.3d 193, 205–06 (D.C. Cir. 2013) 18.3.4
United States v. Lovasco, 431 U.S. 783 (1977) 31.1.1
United States v. LSL Biotechnologies, 379 F.3d 672, 679–80 (9th Cir. 2004) 29.7
United States v. Martin Linen Supply Co, 430 U.S. 564 (1977) 1.2.2
United States v. Mass. Inst. of Tech, 129 F.3d 681 (1st Cir. 1997) 37.5
United States v. Maxwell, 20-cr-00330, Order, ECF No. 28 (S.D.N.Y., 23 July 2020)(D) 39.1.2
United States v. McLellan, 959 F.3d 442, 470–71 (1st Cir. 2020) 29.5
United States v. McVicker, 979 F. Supp. 2d 1154, 1171 (D. Or. 2013) 29.3
United States v. Meregildo, 883 F. Supp. 2d 523 (S.D.N.Y. 2012) 39.2.1
United States v. Mikerin, No. 14-cr-529-TDC (D. Md. 31 August 2015) 29.10
United States v. Manafort et al., No. 1:17-CR-00201-ABJ (D.D.C. filed 8 November 2017), ECF No. 38 ..... 39.1.2
United States v. Manafort, No. 1:18-cr-00083-TSE (E.D. Va. filed 21 June 2018), ECF No. 87 ..... 39.1.3
United States v. Manafort, No. 1:18-cr-00083-TSE (E.D. Va. filed 17 July 2018), ECF No. 138 ..... 39.1.2
United States v. Napout et al., 18-2750-cr, 18-2820-cr (CON) (2d. Cir. argued 7 November 2019) 29.5
United States v. Napout, 963 F.3d 163, 179 (2d Cir. 2020) 29.1
United States v. Neely, 429 F. Supp. 1215, 1225 n.9 (D. Conn. 1977) 18.3.4
United States v. Newman, 659 F.3d 1235 (9th Cir. 2011) 26.2.1
United States v. Nobles 422 U.S. 225 (1975) 37.1.2, 37.3.1, 37.7
United States v. Odebrecht S.A., No. 16-cr-643 (RJD) (E.D.N.Y. 29 January 2020), ECF 17033.5.2
United States v. Ogbazion, 2012 WL 4364306, at *1 (S.D. Ohio 24 September 2012) 35.2.1
United States v. Pac. Gas & Elec. Co, No. 14–CR–00175–TEH, 2015 WL 9460313 (N.D. Cal. 23 December 2015) 1.1.2
United States v. Pac. Gas & Elec. Co, No. 14–CR–00175–TEH, 2016 WL 6804575 (N.D. Cal. 17 November 2016) 1.1.2
United States v. Parse, 789 F.3d 83 (2d Cir. 2015) 39.2.2
United States v. Patel, No. 09-cr-335 (D.D.C. 12 August 2011), ECF No. 434 ..... 29.8
United States v. Percoco, 16 Cr. 776 (VEC) (S.D.N.Y. 11 December 2017) 16.5
United States v. Plaza Health Labs, Inc., 3 F.3d 643, 648 (2d Cir. 1993) 29.3
United States v. Pomeroy, 822 F.2d 718, 720 nn.3-4 (8th Cir. 1987) 18.3.2
United States v. Porcaro, 648 F.2d 753 (1st Cir. 1981) 39.1.3
United States v. Powell, 379 U.S. 48 (1964) 11.3
United States v. Prevezon Holdings, Ltd., 251 F. Supp. 3d 684, 694 (S.D.N.Y. 10 May 2017) 29.10
United States v. Rajaratnam, 708 F. Supp. 2d 371 (S.D.N.Y. 2010) 39.1.1
United States v. Roberts, 660 F. 3d 149 (2d Cir. 2011) 16.5
United States v. Rolls–Royce PLC, No. 16–0247 (S) (S.D. Ohio 20 December 2016) 33.5.2
United States v. Rosemond, 841 F.3d 95, 109–10 (2d Cir. 2016) 18.4.2.1
United States v. Ruehle, 583 F.3d 600 (9th Cir. 2009) 6.4, 37.3.1
United States v. Saechao, 418 F.3d 1073 (9th Cir. 2005) 18.4.3.1
United States v. Saena Tech Corp., 140 F. Supp. 3d 11 (D.D.C. 2015) 24.4.1
United States v. Santos, 553 U.S. 507 (2008) 29.10
United States v. Schwimmer, 892 F.2d 237 (2d Cir. 1989), cert. denied, 502 U.S. 810 (1991) 18.4.4, 37.1.3, 39.1.6
United States v. Sci. Applications Int'l Corp., 555 F. Supp. 2d 40 (D.C. Cir. 2008) 1.1.2

© Law Business Research 2021

United States v. Sec. Nat'l Bank, 546 F.2d 492 (2d Cir. 1976) 1.2.2
United States v. Shkreli, No. 1:15–cr–637 (E.D.N.Y. 3 June 2016), ECF No. 60 ..... 39.3.1
United States v. Shkreli, No. 1:15–cr–637 (E.D.N.Y. 4 August 2017), ECF No. 305 ..... 39.3.1
United States v. Shkreli, No. 1:15–cr–637 (E.D.N.Y. 5 July 2017) 39.3.1
United States v. Siemens Aktiengesellschaft, Information, 12 December 2008 ..... 46.7
United States v. Singh, 518 F.3d 236 (4th Cir. 2008) 1.1.2
United States v. Sitzmann, 893 F.3d 811, 822 (D.C. Cir. 2018) 29.4
United States v. Sociedad Química y Minera de Chile, S.A., No. 1:17-cr-00013 ..... 43.4
United States v. Sota, 948 F.3d 356, 358–59, 361–62 (D.C. Cir. 2020) 29.3
United States v. Stein, No. 93-cr-375, 1994 WL 285020, at *4–5 (E.D. La. 23 June 1994) 29.10
United States v. Stein, 541 F.3d 130 (2d Cir. 2008) 14.1
United States v. Stepney, 246 F. Supp. 2d 1069 (N.D. Cal. 2003) 37.1.3
United States v. Stewart, No. 15CR287, 2016 U.S. Dist. LEXIS 103516 (S.D.N.Y. 22 July 2016) 2.3.3
United States v. Stokes, 726 F.3d 880, 889 (7th Cir. 2013) 18.3.3
United States of America v. Stone, No. 1:19-cr-00018-ABJ (D.D.C.), ECF No. 36 ..... 39.2.2
United States v. Suarez, 791 F.3d 363, 366-67 (2d Cir. 2015) 18.3.3
United States v. T.I.M.E.–D.C, Inc., 381 F. Supp. 730 (W.D. Va. 1974) 1.1.2
United States v. Toohey, 448 F.3d 542 (2d Cir. 2006) 31.2.4
United States v. Transp. Logistics Int'l, Inc., No. 8:18-cr-00011-TDC, ECF No. 10 (D. Md. 2 April 2018) 24.4.1
United States v. Treacy No. S2 08 CR 366 (JSR), 2009 WL 812033 (S.D.N.Y. 24 Mar. 2009) 37.4
United States v. Triumph Capital Group, 544 F. 3d 149, 161 to 165 (2d Cir. 2008) 16.5
United States v. Ubaldo, 859 F.3d 690, 700–01 (9th Cir. 2017) 29.4
United States v. United Shoe Mach. Corp., 89 F. Supp. 357 (D. Mass. 1950) 37.1.1
United States v. US Bancorp, No. 18-CR-150, ECF No. 9 (S.D.N.Y. 22 February 2018) 24.4.1
United States v. Valenzuela, 849 F.3d 477, 484–85 & n.3 (1st Cir. 2017) 29.4
United States v. Vasquez, 899 F.3d 363, 374, No. 17–50564, 2018 WL 3746809 (5th Cir. 7 August 2018) 29.3, 29.4
United States v. Vella, 2011 WL 652752 (3d Cir. 2011) 16.5
United States v. Vilar, 729 F.3d 62, 77 n.11 (2d Cir. 2013) 29.2.2, 29.3
United States v. Walton, 814 F.2d 376, 380 (7th Cir. 1987) 18.3.2
United States v. Weingold, 69 Fed. Appx. 575 (3d Cir. 2003) 37.1.1.1
United States v. Weissman, 195 F.3d 96, 100 (2d Cir. 1999) 18.4.4, 37.1.3
United States v. Weitzenhoff, 35 F.3d 1275 (9th Cir. 1993) 1.1.2
United States v. Wells Fargo Bank, N.A, 132 F. Supp 3d 562–63 ..... 37.1.1.1
United States v. Wells Fargo Bank, N.A, 132 F. Supp. 3d 558, 566 (S.D.N.Y. 2015) 37.1.1.1
United States v. West, 392 F. 3d 450 (D.C. Cir. 2004) 37.1.1.1
United States v. Zarrab, 15-CR-867, 2016 WL 3681423, at *7 (S.D.N.Y. 16 July 2016) 18.2.1
United States v. Zolin, 491 U.S. 554 (1989) 37.1.1.1
United States v. ZTE Corp., No. 17–0120–K (N.D. Tex. 22 March 2017) 33.4
Upjohn Co v. United States, 449 U.S. 383 (1981) 2.3.3, 6.4, 7.8, 7.15, 8.3, 14.3.1, 14.8, 15.2.3, 16.2.3, 18.4.2.2, 37.1.1, 37.1.3, 37.3.1, 37.3.2, 37.4.1, 41.4
Upromise, Inc., In re, FTC File No. 102-3116, No. C-4351 (F.T.C. 27 March 2012), 2012 WL 1225058 ..... 41.5.3
Vannoy v. Celanese Corp., ARB No. 09–118, ALJ No. 2008–SOX–064 (ARB 28 September 2011) 20.1.1
Veon Ltd. Sec. Litig., In re, 2018 WL 4168958, at *1 (S.D.N.Y. 30 August 2018) 24.5.4

© Law Business Research 2021

Verble v. Morgan Stanley Smith Barney, LLC, No. 3:14–CV–74, 2015 WL 8328561 (E.D. Tenn. 8 December 2015) 20.3.1
Vitamins Antitrust Litigation, In re, No. MC 99–197, 2002 U.S. Dist. LEXIS 26490, 2002 WL 35021999 (D.D.C. 23 January 2002) 37.7.2
Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Products Liability Litigation, In re, 3:15–mc–02672–CRB (N.D. Cal. 17 May 2017) 24.6.1
Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Prods. Liab. Litig., In re, Nos. 15-cv-6167, 15-cv-6168, 16-cv-190, 16-cv-184, 2017 WL 66281, at *3–4 (N.D. Cal. 4 January 2017) 29.2.2
Volkswagen "Clean Diesel" Marketing, Sales Practices, and Product Liability Litigation, In re, _ F. Supp. 3d _ 2020 WL 4905093, at *11 (N.D. Cal. 20 August 2020) 29.2.2
Wachovia Bank, N.A, In re, (Department of Justice 16 March 2010) 24.4.1
Walker v. Wilburn, 2015 WL 5873392, at *4 (N.D. Tex. 5 October 2015) 35.2.1
Wal–Mart Stores Inc. v. Indiana Elec.Workers Pension Fund Trust IBEW, 95 A.3d 1264 (Del. 2014) 6.3, 37.1.1.2
Walmart Inc., In the Matter of, File No. 3-19207 (20 June 2019); DOJ Non-Prosecution Agreement, U.S. v. Walmart (20 June 2019) 11.5.5
Walt Disney Co. Derivative Litig., In re, 907 A.2d 693, 745 (Del. Ch. 2005), aff'd, 906 A.2d 2 (Del. 2006) (Disney) 43.2, 43.2.1, 43.3.1, 43.3.2
Walters v. Deutsche Bank, et al, 2008–SOX–70, slip op. at 41 (ALJ 20 March 2009) 20.2.3
Wanamaker v. Columbian Rope Co, 108 F.3d 462 (2d Cir. 1997) 20.2.3
Waterford Tp. Police & Fire Ret. Sys. v. Smithtown Bancorp, Inc., 2014 WL 3569338 (E.D.N.Y. 18 July 2014) 24.5.4
Wayte v. United States, 470 U.S. 598 (1985) 31.1.1
Weatherford v. Bursey, 429 U.S. 545 (1977) 31.1.1
Welch v. Cardinal Bankshares Corp., ARB No. 05–064, ALJ No. 2003–SOX–15 (ARB 31 May 2007) 20.1.1
Welch v. Chao, 536 F.3d 269 (4th Cir. 2008) 20.1.1
Welland v. Trainer, No. 00 Civ. 0738(JSM), 2001 WL 1154666 (S.D.N.Y. 1 October 2001) 37.3.3
Wells Fargo & Co. S'holder Derivative Litig., In re, 282 F. Supp. 3d 1074, 1082 (N.D. Cal. 2017) 43.3.1, 43.6
Wells Fargo Bank, N.A, In re, (Department of Justice 8 December 2011) 24.4.1
Westinghouse Elec. Corp. v. Republic of the Philippines, 951 F.2d 1414 (3d Cir. 1991)37.5, 37.7.2
Wiest v. Lynch, 710 F.3d 121 (3d Cir. 2013) 20.1.1
Wultz v. Bank of China Ltd, 61 F. Supp. 3d 272, 279 (S.D.N.Y. 2013) 35.3.1.2
Wultz v. Bank of China, the Southern District of New York 304 F.R.D. 384 (S.D.N.Y. 2015) 37.3.1
Wylie v. Marley Co, 891 F.2d 1463 (10th Cir. 1989) 37.2
Yahoo! Customer Data Security Breach Litigation, In re, 313 F. Supp. 3d 1113, 1128 (N.D. Cal. 2018) 41.5.3
Yick Wo v. Hopkins, 118 U.S. 356 (1886) 31.1.1
Young v. United States ex. Rel. Vuitton et Fils S.A, 481 U.S. 787 (1987) 31.1.1
Zanazanian v. United States, 729 F.2d 624, 626 (9th Cir. 1984) 18.3.2
Zappos.com, Inc., In re, No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3–4 (D. Nev. 9 September 2013) 41.5.3

Australia

Baker v. Campbell [1983] HCA 39; 153 CLR 52; 57 ALJR 749; 49 ALR 385; (1983) ATC 4606; 14 ATR 713 ..... 36.2.3, 36.7.2

© Law Business Research 2021

Bulk Materials (Coal Handling) Services Pty Ltd v. Coal and Allied Operations Pty Ltd (1988) 13 NSWLR 689 ..... 36.5
Daniels Corporation International Pty Ltd v. Australian Competition and Consumer Commission (2002) 213 CLR 543 ..... 36.7.2
Esso Australia Resources Ltd v. Commissioner of Taxation (1999) 201 CLR 49 ..... 36.4.3
Grant v. Downs, 135 CLR 674 ..... 36.4
Network Ten Ltd v. Capital Television Holdings Ltd (1995) 35 NSWLR 275, 282, Supreme Court of New South Wales 36.5
Newcrest Mining (WA) Ltd v. Commonwealth of Australia (1993) 113 ALR 370, 372, Australian Federal Court 36.5
Ritz Hotel Ltd v. Charles of the Ritz Ltd (No. 4) (1987) 14 NSWLR 100, 101–2 ..... 36.3.2.1
Waterford v. Commonwealth of Australia (1987) 163 CLR 54 ..... 36.3.2.1

European Court of Human Rights

A and B v. Norway (App. nos. 24130/11 and 29758/11) 15 November 2016 (GC) 1.2.4.2
Grande Stevens v. Italy (App. nos. 18640/10, 18647/10, 18668/10 and 18698/10) 4 March 2014 ..... 1.2, 1.2.4.1

European Court of Justice

AY case. *See* Županijski Sud u Zagrebu, Request for preliminary ruling from (C–268/17)
Akzo Nobel Chemicals Ltd v. European Commission (C–550/07 P) EU:C:2010:512, 2010 E.C.R. I–08301 ..... 7.7, 36.3.2.1
Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/1) 40.1, 40.2.7
Di Puma v. Commissione Nazionale per le Società e la Borsa (Consob); Commissione Nazionale per le Società e la Borsa (Consob) v. Zecca (C–596/16 and C–597/16) EU:C:2018:192, 20 March 2018 ..... 1.2.4.2
Garlsson Real Estate SA v. Commissione Nazionale per le Societa e la Borsa (Consob) (C–537/16) EU:C:2018:193; [2018] 3 WLUK 446; [2018] 3 CMLR 11 ECJ (GC) 1.2.4.2
Kossowski, Criminal Proceedings against (C–486/14) EU:C:2016:483; [2016] 1 WLR 4393 ECJ (GC) 1.2.4.2, 23.1
Ricucci matter. *See* Garlsson Real Estate SA v. Commissione Nazionale per le Societa e la Borsa (Consob) (C–537/16)
Schrems II. *See* Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems
Županijski Sud u Zagrebu, Request for preliminary ruling from (C–268/17) EU:C:2018:602, 25 July 2018 ..... 1.2.6

Hong Kong

CITIC Pacific v. Secretary of State for Justice [2012] 2 HKLRD 701 (HK CA) 36.3.2.2, 36.7.1, 36.8.1

New Zealand

Unilateral Investments v. VNZ Acquisitions Ltd [1993] 1 NZLR 468, 476, 478 (High Court) 36.5

Singapore

Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v. Asia Pacific Breweries (Singapore CA) Pte Lte [2007] 2 SLR 367 ..... 36.3.2.2, 36.9.1

© Law Business Research 2021

Table of Legislation

TABLE OF UK LEGISLATION

Statutes

1889 Public Bodies Corrupt Practices Act (c.69)
s.1(2) 25.15
1906 Prevention of Corruption Act (c.34)
s.1 ..... 23.4, 25.15
1965 Criminal Procedure (Attendance of Witnesses) Act (c.69)
s.2 ..... 7.11
1967 Misrepresentation Act (c.7)
s.2(1) 34.5
1968 Civil Evidence Act (c.64)
s.11 ..... 34.7.1
1972 European Communities Act (c.68)
Sch.2 para.1(1)(d) 44.3.1
1977 Criminal Law Act (c.45) 28.6.2
s.1 ..... 9.7, 23.4, 28.2.2, 28.6.2
(1) 28.6.2
s.1A 28.6, 28.6.2
(6) 28.6.2
s.5 ..... 28.6.1
(2) 28.6.2
1979 Customs and Excise Management Act (c.2) 28.5, 44.4
1980 Magistrates' Court Act (c.43)
s.8A 38.5.2.2
1981 Contempt of Court Act (c.49)
s.1 ..... 38.5.2.2
s.2 ..... 38.5.2.2
s.4(1) 38.5.2.2
(2) 38.5.2.2
1981 Senior Courts Act (formerly Supreme Court Act) (c.54)
s.37(1) 30.1.4
1981 British Nationality Act (c.61) 28.2.1
1983 Representation of the People Act (c.2)
s.113 ..... 25.15
1984 Police and Criminal Evidence Act (c.60) 3.5.2.1, 11.2.2, 17.3.6, 17.4.1

© Law Business Research 2021

s.11 ..... 11.2.2
s.14 ..... 17.3.6
s.15(6) 17.3.6
s.24 ..... 17.3.5
s.66 ..... 15.4.1
s.67(9) 7.9
s.78 ..... 15.3.1
Codes of Practice 15.4.1
Code B 17.3.6
Code C 15.5, 17.3.5, 17.4.1
para.6 ..... 17.3.5
para.6.12 ..... 17.3.5
para.10.1 ..... 7.9, 15.4.1
para.10.5 ..... 15.4.1
para.13 ..... 17.3.5
Code D 17.4.1
Code G 17.3.5
1985 Companies Act (c.6)
s.1 ..... 9.7
s.3 ..... 9.7
s.221 ..... 23.2.1.3
s.225 ..... 23.2.1.3
1985 Prosecution of Offences Act (c.23)
Pt II 25.6, 30.1.7
s.16 ..... 25.6
ss.16–19B 25.6, 30.1.7
s.17 ..... 25.6
1985 Administration of Justice Act (c.61)
s.33 ..... 36.3.2.1
1986 Drug Trafficking Offences Act (c.32)
s.9 ..... 17.3.4
1986 Insolvency Act (c.45)
s.423 ..... 36.7.1
1986 Company Directors Disqualification Act (c.46) 25.7
ss.2–5A 25.7
s.2(1) 25.7
s.5A 25.7
(2) 25.7
s.8 ..... 25.7
(2) 25.7
s.21 ..... 25.7
1987 Criminal Justice Act (c.38) 11.2.2, 28.6.2
s.1 ..... 15.3
(3) 1.2.3
s.2 ..... 3.5.2.1, 3.5.2.2, 9.1, 11.2.1, 11.5.2, 12.2, 15.3.2, 15.3.3, 17.3.5, 17.3.7, 44.4
(2) 11.2.1
(3) 11.2.1

© Law Business Research 2021

(9) 15.3.3
(13) 11.2.1
(16) 5.6.1
s.2A 11.2.1
s.3(5) 9.9.3
s.11 ..... 38.5.2.2
s.12 ..... 28.6.1
1988 Criminal Justice Act (c.33) 30.1.1
s.2 ..... 28.1
s.78 ..... 17.3.4
s.159 ..... 38.5.1.2
1988 Copyright, Designs and Patents Act (c.48)
s.280 ..... 36.3.2.1
s.284 ..... 36.3.2.1
1989 Official Secrets Act (c.6) 41.2.1.2
s.1 ..... 41.2.1.2
1990 Computer Misuse Act (c.18) 41.2.1.1
s.1 ..... 19.4.1, 41.2.1.1
s.2 ..... 41.2.1.1
s.3ZA 41.2.1.1
s.3 ..... 41.2.1.1
s.4 ..... 41.2.1.1
1990 Courts and Legal Services Act (c.41)
s.63 ..... 36.3.2.1
1993 Criminal Justice Act (c.36) 28.6
Pt 1 ..... 28.6.2
s.3(2) 28.6.1
1994 Criminal Justice and Public Order Act (c.33)
s.34(1) 15.4.1
(2) 15.4.1
1994 Drug Trafficking Act (c.37)
s.27 ..... 17.3.4
1996 Employment Rights Act (c.18) 19.1, 19.2.1
Pt V 34.6.4
s.43J 19.2.3
s.47B 34.6.4
(1) 19.2.1.3
s.111A 7.12
s.230(3) 19.2.1
1996 Arbitration Act (c.23)
s.9 ..... 34.2.1
ss.33–34 ..... 34.2.2
s.45 ..... 34.2.2
s.103(3) 34.6.5
1996 Criminal Procedure and Investigations Act (c.25) 36.9.3
s.8 ..... 36.9.3
s.37 ..... 38.5.2.2
s.41 ..... 38.5.2.2
1998 Public Interest Disclosure Act (c.23) 2.3.4, 19.1, 19.2.1, 34.6.4

© Law Business Research 2021

s.17 ..... 2.3.4
s.18 ..... 2.3.4
1998 Data Protection Act (c.29) 19.3.4.1, 34.6.7, 40.2.3, 41.2.1.2
1998 Crime and Disorder Act (c.37) 38.6
s.51 ..... 38.5.2.2
s.51A 38.5.2.2
Sch.3 para.3 ..... 38.5.2.2
1998 Criminal Justice (Terrorism and Conspiracy) Act (c.40)
s.5 ..... 28.6.2
1998 Competition Act (c.41) 34.7.1, 34.9, 36.4.2
1998 Human Rights Act (c.42) 17.4.4.1, 25.10, 38.5.1.1
1999 Access to Justice Act (c.22) 25.6, 30.1.7
2000 Powers of Criminal Courts (Sentencing) Act (c.6) 30.1.5
s.130 ..... 30.1.5
(1) 25.2
(3) 25.2
(4) 25.2
(11) 25.2
(12) 25.2
s.131 ..... 30.1.5
2000 Financial Services and Markets Act (c.8) 2.3.2, 2.4.6, 3.4.4, 3.5.2.2, 9.1, 11.2.3.1, 15.3, 19.2.4, 30.2, 34.5, 44.5.2.1, 46.3.1
Pt IVA 25.12, 30.2, 44.5.2.1
Pt XI 17.3.7
s.1B(1)–(3) 25.12
s.19 ..... 25.12
s.26 ..... 34.5
s.27 ..... 34.5
s.30 ..... 34.5
s.31 ..... 11.2.3.1
(1)(a) 25.12
s.55J 25.12
(1)(a) 25.12
(b) 25.12
s.55L 19.3.3, 25.12
s.55M(5) 19.3.3
s.56 ..... 25.13
s.59ZA 42.2.7
s.63E 42.2.7
s.66 ..... 25.13
s.66A 42.2.7
s.90 ..... 34.5
s.90A 34.5
s.117(3) 5.6.1
s.132 ..... 30.3
s.138D 34.5
s.158 ..... 46.4.1.3
s.165 ..... 9.1, 11.2.3.1, 15.3.2, 44.4

© Law Business Research 2021

s.166 2.4.4, 3.5.2.2
s.167 11.2.3.1
s.168 9.1, 11.2.3.1
s.169 11.2.3.1, 11.5.4
(4) 11.5.4
s.171 3.5.2.1, 9.1, 17.3.5, 44.4
ss.171–173 11.2.3.1
s.172 9.1, 44.4
s.173 9.1
s.175 11.2.3.1
s.348 11.2.3.3, 27.2
ss.348–353 2.3.2
s.349 9.9.3
s.382(2) 25.14
s.384 34.3.6
s.393 30.3
(1) 30.3
(4) 30.3
(11) 30.3
s.401 25.11
s.402 25.11
s.404 34.3.6
ss.404A–404G 34.3.6
s.404F(7) 34.3.6
s.413 11.2.3.1, 11.4
Sch.10 34.5
2000 Terrorism Act (c.11) 3.4.1
Pt 3 7.3, 9.2
s.19 3.4.1, 44.5.2.1
s.21ZA 3.4.1
s.21A 3.4.1, 5.2
2000 Regulation of Investigatory Powers Act (c.23) 36.7.2, 40.2.9
2000 Freedom of Information Act (c.36) 3.2, 9.9.1, 11.2.4
2001 Anti-Terrorism, Crime and Security Act (c.24) 28.5, 44.2.1
2002 Export Control Act (c.28) 28.5
2002 Proceeds of Crime Act (c.29) 2.3.1, 3.4.1, 9.2, 9.4.3, 11.2.2, 17.3.2, 19.3.4.4, 25.3, 28.3.2, 30.1.1, 44.3.1, 46.4.1.4
Pts 2–4 17.3.1
Pt 5 17.3.1, 23.2.1.1, 25.8, 28.3.2
Pt 6 25.8
Pt 7 7.3, 28.3.1
Pt 8 17.3.2
s.2A 3.5, 23.5, 25.8
s.6 25.3, 30.1.4
(4)(a) 25.3
(b) 25.3
(c) 25.3
(5) 25.3

© Law Business Research 2021

s.7(2) 25.3
s.9 ..... 25.3
s.10 ..... 25.3
(6)(a) 25.3
(b) 25.3
s.13 ..... 25.3
s.40 ..... 25.9
(2)(b) 25.9
(3)(b) 25.9
s.41(2)(3)(a) 25.9
(b) 25.9
(4) 25.9
s.75 ..... 25.3
(2)(a) 25.3
(b) 25.3
(c) 25.3
s.76(2) 25.3
(4) 25.3
(5) 25.3
s.241A 28.3.2
s.266(2) 25.8
s.267 ..... 25.8
s.282A 28.3.2
s.287 ..... 23.2.1.1
s.294 ..... 25.8
s.295 ..... 25.8
(2) 25.8
ss.297A–297E 25.8
s.298 ..... 25.8
s.303B 25.8
s.303J 25.8
s.303K 25.8
s.303L 25.8
s.303O 25.8
ss.303Z1–303Z3 ..... 25.8
ss.303Z9–303Z13 ..... 25.8
s.303Z14 ..... 25.8
s.316 ..... 23.2.1.1
s.327 ..... 28.3.1
(1)(c) 28.3.1
(2A) 28.3.1
ss.327–329 ..... 2.3.1, 28.3.1, 30.1.1
s.328 ..... 28.3.1
(3) 28.3.1
s.329 ..... 28.3.1
(2A) 28.3.1
s.330 ..... 2.4.1, 3.4.1, 5.2, 9.2
ss.330–332 ..... 2.3.1
s.331 ..... 3.4.1, 5.2

© Law Business Research 2021

s.333A 15.3.4, 30.1.1
s.334 ..... 44.3.1
s.335 ..... 3.4.1, 5.2
s.336 ..... 3.4.1
s.338 ..... 5.2
s.340(2) 28.3.2
(3) 28.3.2
(11)(d) 28.3.1
s.345 ..... 11.2.2
s.362 ..... 30.1.3
s.362A(7) 28.3.2
s.362H(5) 28.3.2
(6) 28.3.2
s.362J 30.1.3
s.362S 28.3.2, 30.1.3
s.382(1) 25.14
(6) 25.14
(9) 25.14
s.384 ..... 25.14
s.414 ..... 28.3.2
s.444 ..... 17.3.1
(1)(a) 17.3.1
s.447(1) 17.3.1
(2)(b) 17.3.4
(8) 17.3.1
s.459(2) 17.3.1
Sch.2 ..... 25.3
Sch.7A 28.3.2
para.7(7) 28.3.2
Sch.9 ..... 5.2
2002 Police Reform Act (c.30)
s.103 ..... 17.2
s.104 ..... 17.2
2002 Enterprise Act (c.40)
Pt 9 ..... 9.9.3
2003 Crime (International Co-operation) Act (c.32) 9.9.4, 11.5.2, 11.5.4, 17.2, 17.3.2, 17.3.6, 28.7
Pt 1 ..... 17.2
s.7 ..... 17.2
(2) 11.5.2, 17.2
s.9 ..... 17.3.6
s.15 ..... 28.7
s.16 ..... 17.3.6
s.17 ..... 17.3.6
(3) 17.3.6
s.18 ..... 17.3.6
s.20 ..... 17.3.7
s.24 ..... 17.3.7
s.35 ..... 17.3.2

© Law Business Research 2021

s.36 17.3.2
ss.36–42 17.3.2
Sch.1 28.7
2003 Courts Act (c.39) 38.6
2003 Extradition Act (c.41) 17.4, 17.4.4, 17.4.4.3, 28.7, 28.7.2, 32.4.4, 32.5.2
Pt 1 17.4, 17.4.4, 17.4.4.1, 17.4.4.3, 32.4.4, 32.5.2, 32.5.3
Pt 2 17.4, 17.4.2, 17.4.3, 17.4.4, 17.4.4.1, 17.4.4.3, 32.4.1, 32.5.3
s.2 17.4.1
s.3 17.4.1
s.4 17.4.1
s.11 17.4.4
s.13 18.3.4, 32.3.3
s.19B 17.4.4.3
(2) 17.4.4.3
s.21 17.4.4.1
(1) 17.4.4.1
s.21A 17.4.4.1, 17.4.4.2
(1)(a) 17.4.4.1
s.26(4) 32.4.4
(5) 32.4.4
ss.26–29 17.4.1
s.28(5) 32.4.4
s.32 17.4.1
s.64 17.4.1
s.65 17.4.1
s.69 17.4.2
s.70 17.4.2
s.71 17.4.2
s.78 17.4.2
(2) 17.4.2
s.79 17.4.4
s.81 18.3.4, 32.3.3
s.83A 17.4.4.3, 32.4.2, 32.5.1
(2)(b) 32.5.1
s.87 17.4.4.1, 18.3.4
(1) 17.4.4.1
s.103(10) 32.4.4
s.105(5) 32.4.4
s.108(4) 32.4.4
(7A) 32.4.4
s.137 17.4.2
s.138 17.4.2
ss.166–168 17.4.1
s.193 17.4.3
s.194 17.4.3
2003 Criminal Justice Act (c.44) 38.6

© Law Business Research 2021

s.71 ..... 38.5.2.2
s.75 ..... 30.1.4
s.101(1)(g) 15.4.3
s.144 ..... 9.5, 25.5, 30.1
s.164 ..... 25.4, 30.1.2
Sch.2 ..... 30.1.4
2004 Pensions Act (c.35)
s.58A 11.2.5
s.58B 11.2.5
s.72A 11.2.5
2005 Serious Organised Crime and Police Act (c.15) 15.1, 19.4.2, 30.1
Ch 2 ..... 30.1
s.62 ..... 11.2.2, 15.3.2, 17.3.7
s.66 ..... 11.2.2
s.67(1) 11.2.2
s.71 ..... 17.5, 19.4.2
(4) 17.5
ss.71–75 ..... 17.5, 23.2.1.3, 30.1
s.73 ..... 1.2.1, 9.5, 17.5, 19.4.2, 25.5, 30.1, 30.1.1, 36.2.4
s.74 ..... 25.5, 30.1
Sch. 9.5
2006 Fraud Act (c.35) 28.6, 28.6.2, 30.1.1
s.2 ..... 9.7, 28.6.2
s.3 ..... 28.6.2
s.4 ..... 28.6.2
Sch.1 ..... 28.6.2
2006 Companies Act (c.46) 3.1, 40.4, 41.2.1.2, 42.2.1, 42.2.6
Pt 11 ..... 34.4.1
Ch 1 ..... 34.4.1
Pt 30 ..... 34.4.2
s.171 ..... 42.2.1.1
ss.171–177 ..... 5.3, 42.2.1.2
ss.171–178 ..... 42.2
s.172 ..... 3.1, 34.4.1, 42.2.1.2, 42.2.2, 42.2.6
(1) 42.2.6
(a)–(f) 42.2.6
(e) 41.2.1.2
s.173 ..... 42.2.1.3
s.174 ..... 42.2.1.2, 42.2.1.4
(2) 42.2.1.4
s.175 ..... 42.2.1.5
(1) 42.2.1.5
(4)(a) 42.2.1.5
(b) 42.2.1.5
s.176 ..... 42.2.1.6
s.177 ..... 42.2.1.7
s.180(4)(b) 42.2.1.5, 42.2.1.7
s.182 ..... 42.2.1.7
s.250 ..... 25.7

© Law Business Research 2021

s.252 ..... 42.2.1.5, 42.2.1.7
s.414CA 19.2.7
s.465 ..... 42.2.6
s.467 ..... 42.2.6
s.996 ..... 34.4.2
2007 Corporate Manslaughter and Homicide Act (c.19) 1.1.1
s.1 ..... 7.5
2007 Serious Crime Act (c.27) 25.10, 28.5, 28.6.3, 44.3.1
Pt 1 ..... 30.1.3
ss.44–46 ..... 28.6.3
s.52 ..... 28.6.3
Sch.4 ..... 28.6.3
2008 Finance Act (c.9)
Sch.36 ..... 28.7
para.1 ..... 28.7
2008 Counter-Terrorism Act (c.28) 28.5, 44.2.1
Sch.7 para. 12 ..... 3.4.1
2009 Coroners and Justice Act (c.25)
s.125(1) 25.1
2010 Bribery Act (c.23) 1.1.1, 2.3.1, 2.3.2, 3.1, 3.2, 3.5, 3.6.5, 9.4.3, 15.2.1, 19.3.2.1, 23.2.1.1, 23.2.1.2, 23.4, 25.4, 25.15, 28.1, 28.2, 28.4, 28.5, 30.1, 30.1.1, 33.2.2, 42.1, 46.2.3, 46.4.1.1, 46.6, 46.7
s.1 ..... 11.2.1, 25.15, 28.2, 28.2.1, 30.1.1
s.2 ..... 11.2.1, 25.15, 28.2, 28.2.1, 30.1.1
s.6 ..... 11.2.1, 25.15, 28.2, 28.2.1, 30.1.1
s.7 ..... 1.1.1, 1.3.4, 2.3.1, 2.3.2, 3.2, 3.3, 7.5, 9.3, 9.6, 9.8, 11.5.1, 15.2.1, 19.3.2.1, 23.1, 23.2.1.2, 23.4, 25.4, 28.2, 28.2.2, 28.4, 30.1.1, 46.2.1, 46.2.3, 46.4.1.1, 46.7
(1) 46.2.1, 46.4.1.1
(2) 19.3.2.1, 46.2.1
(5) 46.2.1
s.8 ..... 15.2.1
s.9 ..... 1.1.1, 3.2, 46.2.3
(1) 46.4.1.1
s.11 ..... 30.1.1
s.12(2)(b) 28.2.1
(c) 28.2.1
(3) 28.2.1
(4) 28.2.1
(5) 28.2.2
s.14 ..... 28.2.1, 30.1.1
2010 Terrorist Asset Freezing etc. Act (c.38) 3.4.1, 28.5, 44.2.1, 44.4
s.17 ..... 44.2.3
s.19 ..... 3.4.1, 44.4
2012 Legal Aid, Sentencing and Punishment of Offenders Act (c.10) 25.6

© Law Business Research 2021

2012 Financial Services Act (c.21) 30.2
Pt 7 ..... 9.2
2013 Crime and Courts Act (c.22) 3.2, 7.4, 9.4.1, 17.4.4.3, 17.5, 25.16, 32.4.2, 33.2.2, 46.6
Pt I 33.2.2
s.5(3)(e) 33.2.2
s.45 ..... 23.1, 36.2.4
s.48 ..... 28.3.2
s.50 ..... 32.5.1
Sch.17 ..... 13.2.2.1, 17.5, 23.2.1.2, 33.2.2, 36.2.4, 44.5.3
para.5 ..... 23.2.3
(1) 34.7.1
(3) 23.2.1.2
(4) 9.5, 23.2.1.2, 25.16
para.6(1) 9.4.3, 9.4.5
para.7 ..... 23.1
para.8 ..... 23.2.1.2
para.9 ..... 23.1
para.12 ..... 38.5.2.3
para.13(6) 9.2, 17.5
Sch.20 para.6 ..... 35.5.1
2013 Enterprise and Regulatory Reform Act (c.24) 19.2.1.4
s.17 ..... 19.2.1.3
s.19 ..... 19.2.1.4
2013 Defamation Act (c.26) 34.6.4
2013 Financial Services (Banking Reform) Act (c.33) 42.2.7
2015 Serious Crime Act (c.9) 25.10
s.1(3) 25.10
s.5(3)(a) 25.10
(c) 25.10
(e) 25.10
(f) 25.10
s.5(5)(a) 25.10
s.11 ..... 25.10
s.19(5) 25.10
s.35(1) 25.10
2015 Modern Slavery Act (c.30)
s.54 ..... 19.2.7
2016 Investigatory Powers Act (c.25) 40.2.9
s.3(1) 19.4.1, 41.2.1.1
2017 Policing and Crime Act (c.3) 28.5, 44.3.1, 44.3.2
s.144 ..... 28.5
s.145 ..... 28.5
s.146 ..... 28.5
(3) 44.3.2
s.147 ..... 44.5.3
s.149(2) 28.5
s.150 ..... 28.5
s.151 ..... 28.5

© Law Business Research 2021

2017 Criminal Finances Act (c.22) 1.1.1, 3.4.2, 7.5, 9.3, 9.6, 19.3.2.2, 23.1, 28.4, 30.1.3, 42.1, 46.2.2, 46.2.3, 46.4.1.2
Pt 1 ..... 28.3.2, 30.1.3
Pt 3 ..... 1.1.1, 2.3.1, 9.3, 28.4
s.1 ..... 28.3.2
ss.1–9 ..... 25.8, 30.1.3
s.3 ..... 28.3.2
s.9 ..... 28.1
s.13 ..... 28.3.2
s.44(2) 28.4, 46.2.2
(3) 28.4, 46.2.2
(4) 28.4
(6) 28.4
ss.44–52 ..... 2.3.1,
s.45 ..... 3.2, 3.4.2, 7.5, 19.3.2.2, 28.4, 46.2.2, 46.4.1.2
(2) 46.2.2
s.46 ..... 3.2, 3.4.2, 7.5, 19.3.2.2, 28.4, 46.2.2, 46.4.1.2
(2) 28.4, 46.2.2
(3) 46.2.2
s.47(1) 46.4.1.2
s.362E 30.1.3
2018 Data Protection Act (c.12) 7.14, 30.1, 38.5.4, 40.1, 40.2, 40.2.1, 40.2.3, 40.2.5, 40.2.6, 40.4.2, 40.6.2, 41.2.1.1, 41.2.1.2
Pt 2 ..... 41.2.1.2
Pt 6 ..... 11.2.4
s.10 ..... 40.2.5
s.45 ..... 40.6.2
s.67 ..... 5.2
s.142(1) 11.2.4
s.143(4) 11.2.4
s.155(1)(b) 11.2.4
s.170 ..... 19.4.1
ss.170–173 ..... 41.2.1.1
s.196 ..... 19.4.1
Sch.1 Pt 1 ..... 40.2.5
Pt 2 ..... 40.2.6
2018 Sanctions and Anti-Money Laundering Act (c.13) 28.5, 44.2.1
Pt 2 ..... 28.7.3
s.11 ..... 44.6.2
s.12 ..... 44.6.2
s.15 ..... 44.6.2
s.23 ..... 44.6.2
s.21 ..... 28.5
ss.49-50 ..... 28.7.3
s.51 ..... 28.1
2018 European Union (Withdrawal) Act (c.16) 41.2.1.2
2019 Crime (Overseas Production Orders) Act (c.5) 1.3.2, 5.6.4, 11.5.2, 12.6, 17.3.7, 28.7

© Law Business Research 2021

s.2(1)(a) 17.3.7
s.3 17.3.7
s.4 17.3.7
2020 Coronavirus Act (c.7) 18.3.2, 38.6
ss.53–57 18.3.2
Sch.25 para.85A(1) 38.6
(2) 38.6
2020 Extradition (Provisional Arrest) Act (c.18) 32.5.2
Sch.A1 32.5.2

Statutory Instruments

1986 Costs in Criminal Cases (General) Regulations (SI 1986/1335) 25.6, 30.1.7
1990 Criminal Justice (Confiscation) (Northern Ireland) Order (SI 1990/2588)
art.14 17.3.4
1996 Proceeds of Crime (Northern Ireland) Order (SI 1996/1299)
art.32 17.3.4
1998 Civil Procedure Rules (SI 1998/3132) 34.2.1, 34.3, 34.3.1, 34.3.3, 34.4.1
r.3.1(2)(f) 34.2.1
r.7.3 34.3.3
r.19.1 34.3.3
r.19.7 34.3.1
Pt 31 36.8.3
r.31.19(6) 36.9.3
r.31.20 36.8.3
r.31.22 34.7.3
PD 51M 34.3.4
PD 51U 34.7.3, 36.8.3
(19) 36.8.3
2000 Telecommunications (Lawful Business Practice) (Interception of Communications)
Regulations (SI 2000/2699) 40.2.9
2003 Proceeds of Crime Act 2002 (Financial Threshold for Civil Recovery)
Order (SI 2003/175) 23.2.1.1
2003 Privacy and Electronic Communications (EC Directive) Regulations
(SI 2003/2426) 9.4.2, 41.2.1.2
2003 Extradition Act 2003 (Designation of Part 1 Territories) Order (SI 2003/3333) 17.4, 32.5.2
2003 Extradition Act 2003 (Designation of Part 2 Territories) Order (SI 2003/3334) 17.4
2005 Extradition Act 2003 (Parties to International Conventions) Order (SI 2005/46) 17.4.3
2005 Proceeds of Crime Act 2002 (External Requests and Orders) Order
(SI 2005/3181) 17.3.1, 17.3.3, 17.3.4
art.6 17.3.1
art.7 17.3.1
art.8 17.3.1
art.18 17.3.4
art.20 17.3.4
art.21 17.3.4
(6) 17.3.4
art.22 17.3.4
art.25 17.3.4

© Law Business Research 2021

art.26 ..... 17.3.4
art.202 ..... 17.3.3
art.203 ..... 17.3.3
2006 Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order (SI 2006/1070) 28.3.1
2007 Money Laundering Regulations (SI 2007/2157) 3.4.1, 46.3.1
2008 Export Control Order (SI 2008/3231) 28.5
Pt 4 ..... 28.5
Sch.1 ..... 28.5
2014 Proceeds of Crime (External Investigations) Order (SI 2014/1893)
Pt 5 ..... 17.3.2
art.30 ..... 17.3.2
2015 Public Contracts Regulations (SI 2015/102) 3.2, 23.2, 25.15, 25.16
reg.5 ..... 25.15
(1) 25.15
(8) 25.15
(12) 25.15
(15) 3.2, 25.15
2015 Criminal Procedure Rules (SI 2015/1490) 23.4, 32.4.4, 38.5.1.1
r.3.3 ..... 23.2.1.3
r.5.8 ..... 23.4
r.6.2(1) 38.5.1.1
r.11.2(3)(c) 23.4
r.15.3 ..... 36.9.3
r.15.5 ..... 36.9.3
2016 Companies, Partnerships and Groups (Accounts and Non-Financial Reporting) Regulations (SI 2016/1245) 19.2.7
2017 Democratic People's Republic of Korea (European Union Financial Sanctions Regulations (SI 2017/218) 44.2.1
2017 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (SI 2017/692) 3.4.1
reg.3(1) 46.2.4
reg.8 ..... 3.4.1, 46.2.4
reg.19 ..... 3.4.1
reg.20 ..... 3.4.1
reg.86 ..... 46.2.4, 46.4.1.4
(3) 46.2.4
2017 Criminal Justice (European Investigation Order) Regulations (SI 2017/730) 1.3.2, 9.9.4, 28.7.1
2018 Network and Information Systems Regulations (SI 2018/506) 41.2.1.2
reg.1 ..... 41.2.1.2
2018 Companies (Miscellaneous Reporting) Regulations (SI 2018/860) 42.2.1.2, 42.2.6
2018 EU Market Abuse Regulation and the Market Abuse (Amendment) (EU Exit) Regulations (Draft) 9.2
2019 Russia (Sanctions) (EU Exit) Regulations (SI 2019/855) 44.6.2
reg.28 ..... 44.6.2
reg.37 ..... 44.6.2
reg.44 ..... 44.6.2
reg.52 ..... 44.6.2

© Law Business Research 2021

2019 Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations (Draft) 44.2.4.1
2020 Extradition Act 2003 (Amendments to Designations) Order (SI 2020/265) 32.4.1
2020 Global Human Rights Sanctions Regulations (SI 2020/680) 28.5, 44.6.2
reg.6(3) 28.5
2020 Criminal Procedure Rules (SI 2020/759) 32.4.4

TABLE OF US LEGISLATION

CONSTITUTION

1st Amendment 33.5.5, 39.1.1, 39.1.2
5th Amendment 1.2, 1.2.2, 2.4.1, 11.3, 11.5.1, 12.4, 16.5, 18.4.2.2, 18.4.3.1, 18.5.3, 35.2.2, 35.4.4
Double Jeopardy Clause 1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.6
6th Amendment 14.3, 31.2.1, 31.2.5.1, 39.1.1, 39.1.3, 39.3.1
Speedy Trial Clause 18.3.2
8th Amendment 31.2.5.2
14th Amendment 39.1.1
Due Process Clause 39.1.2

FEDERAL LEGISLATION

Federal Acts

1863 False Claims Act (31 U.S.C. §§ 3729 – 3733) 10, 10.1.2, 10.1.2.3, 20.4, 20.4.1, 20.4.2, 24.4.1, 26.1, 26.3
1890 Sherman Antitrust Act (26 Stat. 209, 15 U.S.C. §§ 1-7) 29.7, 33.2.1, 35.3.3.3, 46.4.2.3
1911 All Writs Act (28 U.S.C. § 1651) 26.5
1914 Federal Trade Commission Act (15 U.S.C. §§ 41–58) 41.2.2.1, 41.5.3
1925 Federal Arbitration Act (Pub.L. 68–401, 43 Stat. 883, 9 U.S.C. § 1) 35.3.1.5
1930 Tariff Act (Pub.L 71–361, 19 U.S.C. 4) 31.2.5.2
1933 Securities Act (Pub.L 73–22, 15 U.S.C. § 77s(c)) 26.3, 35.3.1.4, 43.2
s.19(b) 11.3
s.20(b) 24.2
s.24 ..... 43.4
1934 Securities Exchange Act (Pub.L 73–291, 15 U.S.C. 78a) 20.1.2, 26.3, 29.2, 29.2.2, 29.6, 35.3.1.4, 37.4, 43.2, 43.4
s.10(A) 6.2, 43.6
s.10(b) 29.2, 29.2.1, 29.2.2, 29.3, 29.6
s.10(b)-5 ..... 29.2
s.13(a) 43.4
s.15(b)(4) 24.5.3
s.20(a) 43.4
s.21(a) 37.4
(1) 43.4
(d)(2) 43.4
(3) 43.4
(5) 26.4, 43.4

© Law Business Research 2021

s.21F–4 ..... 43.5
s.32(a) 43.4
1935 National Labor Relations Act (Pub.L 74–198, 29 U.S.C. § 151–169) 14.2
1936 Commodity Exchange Act (Pub.L 74–675, 49 Stat. 1491, 7 U.S.C. 1 § 1) 14.2, 20.1.1, 29.2.2, 29.6
s.22 ..... 29.6
(a) 29.6
s.23 ..... 20.1.2
1938 Fair Labor Standards Act (29 U.S.C. § 203) 14.2
1940 Investment Advisers Act (15 U.S.C. § 80b–1)
s.206(4) 24.5.3
1940 Investment Company Act (Pub.L. 76–768, 15 U.S.C. § 80a–41(b))
s.9(a) 24.5.3
1948 Statute of Limitations (28 U.S.C. § 2462) 26.4
1948 Water Pollution Control Act (33 U.S.C. 1251 – 1376; Ch 758; P.L. 845, June 30, 1948; 62 Stat. 1155) 20.1
1954 Atomic Energy Act (Pub.L. 83–703, 68 Stat. 919, 42 U.S.C § 2011) 20.1
1957 Jencks Act, (18 U.S.C. § 3500) 16.5
1964 Civil Rights Act (Pub.L. 88–352, 78 Stat. 241)
Title VII 14.2
1967 Age Discrimination in Employment Act (29 U.S.C. § 621–634) 14.2
1968 Fair Housing Act (Title VIII of the Civil Rights Act of 1968) (42 U.S.C. 3601–3619) 26.3
1968 Freedom of Information Act (Pub.L. 89–487, 0 Stat. 250 5 U.S.C. 5(II)) .. 11.3, 24.5.2, 33.5.5, 34.3.2, 35.3.1.2
1968 Natural Gas Pipeline Safety Act (Pub.L. 90–481) 1.1.2
1968 Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511(2)(j)) 14.4.2, 40.3
1970 Racketeer Influenced and Corrupt Organizations Act (Pub.L. 91–452, 84 Stat. 941, 18 U.S.C. §§ 1961–1968) 26.7.4, 29.4, 29.5
1970 Bank Secrecy Act (Pub.L. 91–508, 84 Stat. 1118, 12 U.S.C. 13 § 1724, 12 U.S.C. 16 § 1813, 15 U.S.C. 2B § 78a) 4.2.1, 6.2, 24.4.1, 46.5
1970 Occupational Safety and Health Act (Pub.L. 91–596, 84 Stat. 1590, 29 U.S.C. 15 § 651) 14.2
1970 Clean Air Act (Pub.L. 88–206, 77 Stat. 392, 42 U.S.C. 85 § 7401) 20.1
1972 Clean Water Act (Pub.L. 92–500, 86 Stat. 816, 33 U.S.C. 23 § 1151) 1.1.2, 20.1
1973 Rehabilitation Act of 1973, (Pub.L. 93–112, 87 Stat. 355, codified as 29 U.S.C. § 701) 14.5
1974 Speedy Trial Act (88 Stat. 2080, 18 U.S.C. §§ 3161–3174) 24.4.1
1974 Employee Retirement Income Security Act (Pub.L. 93–406, 88 Stat. 829, 29 U.S.C. ch. 18 § 1001 et seq) 10.2.2
1977 Federal Mine Safety and Health Act (Pub. L. 95–164, 91 Stat. 1290, 30 U.S.C. 22 § 801) 20.1
1977 International Emergency Economic Powers Act (Pub.L. 95–223, 91 Stat. 1625, 50 U.S.C. 35 § 1701) 26.7.3, 29.9
1977 Foreign Corrupt Practices Act (Pub. L. 95–213, 15 U.S.C. § 78dd–1) 1.1.2, 2.3.1, 4.1, 4.3.1.1, 6.2, 6.6.1, 10, 10.1.2, 10.1.2.1, 10.1.4, 10.2.1, 10.2.3, 10.2.5, 10.3.2, 10.3.3, 11.3, 11.3.1, 11.5.5, 18.3, 18.3.4, 18.3.5, 18.3.6, 22.13, 23.2.1.2, 24.4.1, 24.6.1, 26.1, 26.2.2, 26.4, 26.6, 26.7.1, 29.8,

© Law Business Research 2021

29.10, 33.3, 33.5.1, 33.5.2, 35.5.2, 37.4.1, 43.4, 46.4.2.1, 46.6

1978 Inspector General Act Pub L. 95–452, 92 Stat. 1101 aka 92 Stat. 1101) 11.3
1982 Foreign Trade Antitrust Improvements Act (96 Stat. 1246, 15 U.S.C. 6a) 29.7
1982 Surface Transportation Assistance Act (96 Stat. 2097) 20.1
49 U.S.C. § 31105 ..... 20.1
1984 Sentencing Reform Act (Part of the Comprehensive Crime Control Act 1984, Pub.L. 98–473, S. 1762, 98 Stat. 1976) 31.2.1
1984 Alternative Fines Act (18 U.S.C. § 3571) 26.2.1, 26.7.1
1984 Bail Reform Act (18 U.S.C. §§ 3141–3150) 18.2.1
1986 Electronic Communications Privacy Act (Title I of the Electronic Communications Privacy Act of 1986) (Pub. L. 99–508, 100 Stat. 1848, 18 U.S. Code § 2515) 40.3
1986 Anti-Kickback Enforcement Act (Pub. L. 99–634,100 Stat. 3523) 4.2.1
1986 Computer Fraud and Abuse Act (18 U.S.C. § 1030) 14.4.1
1986 Stored Communications Act (Title II of the Electronic Communications Privacy Act of 1986) (Pub. L. 99–508, 100 Stat. 1848, 18 U.S.C. §§ 2701–2712) 14.4.1, 40.3
s.2523 ..... 40.5
1986 Money Laundering Control Act (Pub. L. 99–570, 100 Stat. 3207, 18 U.S.C. 46 § 981, 18 U.S.C. 95 § 1956-1957) 29.10
s.1956 ..... 29.10
1988 Employee Polygraph Protection Act (29 U.S.C. 22) 14.4.3
1989 Financial Institutions Reform, Recovery and Enforcement Act (Pub. L. 101–73, 103 Stat. 183) 26.3
1990 Crime Control Act (Pub. L. 101–647, 104 Stat. 4789, 18 U.S.C. § 1) 31.2.6
1990 Americans with Disabilities Act (Pub. L. 101–336, 104 Stat. 327, 42 U.S.C. 126 § 12101) 14.2
1993 Family and Medical Leave Act (Pub. L. 103–3, 107 Stat. 6, 29 U.S.C. § 2601) 14.2, 14.5
1995 Private Securities Litigation Reform Act (Pub. L. 104-67, 109 Stat. 737) 35.3.1.4
1996 Iran Sanctions Act (formerly Iran and Libya Sanctions Act of 1996 (ILSA)) (Pub.L 104-172, 110 Stat. 1541, 50 U.S.C. § 1701) 29.9
1996 Mandatory Victims Restitution Act (Pub. L. No. 104-132, § 204, 110 Stat. 1214, 1227 (18 U.S.C. §§ 3556, 3663 and 3664)) 10.2.3, 31.2.6
1996 Health Insurance Portability and Accountability Act (Pub. L. 104–191, 110 Stat. 1936)
42 U.S.C. § 1301 ..... 6.6.2, 11.3, 41.2.2.1
s.248 ..... 11.3
s.1173 ..... 41.2.2.1
1998 Securities Litigation Uniform Standards Act (Pub. L. 105–353, 112 Stat. 3227) 35.3.1.4
1999 Financial Services Modernization Act (Gramm-Leach-Bliley Act) (Pub.L. 106–102, 113 Stat. 1338, 15 U.S.C. §§ 6801 to 6827) 41.2.2.1
1999 Foreign Narcotics Kingpin Designation Act, (aka Kingpin Act) (Pub.L. 106–120, 113 Stat. 1606) 45.1.1
2001 USA Patriot Act (Pub, L 107-56, 115 Stat. 272 (2001)) 29.11
2002 Sarbanes–Oxley Act (Pub.L. 107–204, 116 Stat. 745) 4.2.1, 6.2, 14.2, 20.1, 20.1.1, 20.2.1, 20.2.3, 20.3.1, 43.2, 43.2.3
s.301 ..... 43.2.3
s.307 ..... 4.5, 6.2
s.806 ..... 14.2, 20.2.3
s.902(a) 43.4

© Law Business Research 2021

s.1107 ..... 14.2
2004 Antitrust Criminal Penalty Enhancement and Reform Act of 2004 (Pub. L. 108-237, title II, June 22, 2004, 118 Stat. 665)
s.213(a) 10.1.2.2
2005 Class Action Fairness Act (Pub. L. 109–2, 119 Stat. 4, 28 U.S.C. §§ 1332(d), 1453, and 1711–1715) 35.3.1.4
2010 Patient Protection and Affordable Care Act ((Pub. L. 111–149, 124 Stat. 119–1025) ... 20.1
2010 Dodd–Frank Wall Street Reform and Consumer Protection Act (Pub.L. 111–203, 124 Stat. 1376–2223) 2.3.4, 14.2, 20.1.1, 20.1.2, 20.2.1, 20.2.3, 20.3.1, 29.2.2, 29.6, 43.2, 43.4, 43.5
s.748 ..... 14.2
s.922 ..... 14.2
s.929P 29.2.2, 29.6
(b) 29.2.2
2010 Consumer Financial Protection Act (Pub.L. 111–203, Title X, 21 July 2010, 124 Stat. 1955, 12 U.S.C. §5536) 14.2
s.1057 ..... 14.2
2012 Moving Ahead for Progress in the 21st Century Act (Pub.L. 112–141, 126 Stat. 405) .20.1
2012 Magnitsky Act (Pub.L. 112–208, 126 Stat. 1496) 28.3.2
2014 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Pub. L. 113-283 ..... 41.2.2.1
2015 Motor Vehicle Safety Whistleblower Act, 49 U.S.C. § 30172 ..... 20.1
2016 Global Magnitsky Human Rights Accountability Act (Global Magnitsky Act, Title XII, Subtitle F of P.L. 114- 328; 22 U.S.C. § 2656 note) 26.7.3, 45.1.1
2017 Countering America's Adversaries Through Sanctions Act (H.R. 3364, Pub. L. 115–44) 45.1.4.6
s.228 ..... 45.1.4.6
s.231 ..... 45.1.4.6
s.232 ..... 45.1.4.6
2017 Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act (83 Fed. Reg. 46347 (10 September 2018)) 26.7.3
2018 Cybersecurity and Infrastructure Security Agency Act (H.R. 3359, Pub.L. 115–278) 41.2.2.1
2018 Clarifying Lawful Overseas Use of Data Act (CLOUD) (Pub.L. 115–141, H.R. 4943) 1.3.2, 12.6, 17.3.7, 40.5
2018 Foreign Investment Risk Review Modernization Act (HR 5841) 22.13.7
2018 First Step Act (Pub.L. 115–391) 31.1.3
2019 Whistleblower Protection Reform Act (HR 2515) 14.2
2019 TRAP Act (HR 4330) 32.5.2
2019 Caesar Syria Civilian Protection Act of 2019 (part of National Defense Authorization Act for Fiscal Year 2020 (HR 2500))
s.7412 ..... 45.1.4.4
(2) 45.1.4.4
2020 Families First Coronavirus Response Act (HR 6201) 14.5

Executive Orders

2014 Exec. Order No. 13662, 79 Fed. Reg. 16167 (20 March 2014) 45.1.4.6
2014 Exec. Order No. 13662, 79 Fed. Reg. 16169-71 (24 March 2014) 45.1.1, 45.1.4.6
2017 Exec. Order No. 13810, 82 Fed. Reg. 44705 (20 September 2017) 45.1.4.3

© Law Business Research 2021

2018 Exec. Order No. 13850, 83 Fed. Reg. 55243 (2 November 2018) 45.1.4.7
2019 Exec. Order No. 13871, 84 Fed. Reg. 20761 (May 10, 2019) 45.1.4.2
2019 Exec. Order No. 13884, 84 Fed. Reg. 38843 (6 August 2019) 45.1.4.7
2020 Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 January 2020) 45.1.4.2

US Code

Title 5: Government Organization and Employees
s.552 ..... 35.3.1.2
Title 6: Domestic Security
s.1501(7)(A)–(B) 41.2.2.1
s.1503(a)(1) 41.2.2.1
(b) 41.2.2.1
(c)(1) 41.2.2.1
(d)(1)–(2) 41.2.2.1
Title 7: Agriculture
s.1a(9) 29.6
s.6(b)(2) 29.6
(c)(1) 29.6
s.9(a)(1) 29.6
(2) 29.6
s.12a(2) 24.5.3
(3) 24.5.3
s.13(a)(2) 29.6
s.15 ..... 11.3
s.26 ..... 14.2, 20.1.1
Title 9: Arbitration
s.1 ..... 35.3.1.5
Title 12: Banks and Banking
s.1785(j) 37.5
s.1828(x) 37.5
s.1833a 26.3
s.5567 ..... 14.2
Title 15: Commerce and Trade
s.1 ..... 29.7
s.6a 29.7
s.15 ..... 35.3.3.3
(a) 10.2.5
s.17t(a) 43.4
s.45(a)(1) 41.2.2.1
s.77a 14.2
s.77p 35.3.1.4
s.77t(b) 26.5
s.77x 43.4
s.78aa(b) 29.2.2
(2) 20.2.4
s.78bb 35.3.1.4
s.78dd–1 ..... 24.4.1, 46.4.2.4
(a) 26.7.1
(f) 43.4

© Law Business Research 2021

ss.78dd–1–78dd–3 ..... 29.8
s.78dd–2 ..... 46.4.2.4
(a) 26.7.1
(d) 26.7.1
(d)(2) 11.3
s.78dd–2(g)(1)(A) 26.7.1
s.78dd–2(g)(2) 26.7.1
(h)(1) 46.4.2.4
s.78dd–3 ..... 29.8
(a) 26.7.1, 29.8
(d) 26.7.1
(e)(1)(A) 26.7.1
(e)(2) 26.7.1
s.78ff(a) 26.7.1, 43.4
(c)(1)(A) 26.7.1
(B) 26.7.1
s.78ff(c)(2)(B) 26.7.1
(3) 26.2.1, 26.7.1
s.78j(b) 29.2.1
s.78j–1 ..... 6.2, 43.6
s.78m 26.7.1, 29.8
(b)(4) 43.4
(5) 43.4
s.78o(b)(4)(B) 24.5.3
s.78t(b) 24.2
s.78u 20.2.3
s.78u(a)(1) 43.4
s.78u(d) 26.5
(1) 26.7.1
(2) 43.4
(3) 26.7.1, 43.4
(5) 43.4
s.78u–1(a) 26.3
s.78u–2(b) 26.3
s.78u–4 ..... 35.3.1.4
s.78u–5 ..... 35.3.1.4
s.78u–6 ..... 20.1.1
(a)(6) 14.2, 20.1.1
(h)(1)(A) 20.1.1
(B)(i) 14.2
(iii)(I)–(II) 14.2
(C) 14.2
s.80a–9(a)(1) 24.5.3
s.7245 ..... 6.2

Title 18: Crimes and Criminal Procedure

s.215 ..... 26.6
s.981 ..... 18.6, 26.6, 26.7.3, 31.2.5.2
(a) 26.2.1
(1)(C) 26.2.1

© Law Business Research 2021

s.982 ..... 18.6, 26.6, 31.2.5.2
(a) 18.6, 26.2.1
(c)(91) 31.2.5.2
(d)(1) 31.2.5.2
s.983(a)(1) 18.6
(4) 18.6
(j) 18.6
s.983–5 ..... 31.2.5.2
s.984(a)(1) 18.6
s.985(b)(1) 18.6
(c) 18.6
s.1001 ..... 11.3
s.1030 ..... 14.4.1, 41.1.1
s.1343 ..... 26.6, 29.5
s.1349 ..... 43.4
s.1513(c) 14.2
s.1514A 20.1.1
(a) 14.2, 20.1.1
(1) 2.3.4
(b)(1)(B) 20.1.1
(c) 14.2
(e)(2) 20.2.3
s.1519 ..... 2.4.1
s.1621 ..... 11.3
s.1956 ..... 26.6, 26.7.2, 26.7.4, 29.10
(a)(1) 29.10
(2) 29.10
(c)(7) 26.2.1
(f) 29.10
(1) 29.10
s.1957 ..... 26.6, 26.7.2, 26.7.4
s.1961 ..... 26.7.4
s.1961(1) 26.7.4
s.1962 ..... 26.7.4, 29.4
(a) 26.7.4
(a)–(c) 29.4
(b) 26.7.4
(c) 26.7.4
(d) 26.7.4
s.1963(a) 26.7.4, 29.4
(d) 26.7.4
(e) 18.6
s.1964(a)–(b) 29.4
(c) 26.7.4, 29.4
s.2510 ..... 14.4.2
(5)(a) 14.4.2
(15) 14.4.1
ss.2510–2522 ..... 40.3
ss.2511–2522 ..... 40.3

© Law Business Research 2021

s.2701 ..... 14.4.1, 40.3
(a) 40.3
ss.2701–2711 ..... 40.3
ss.2701–2712 ..... 40.3
ss.3121–3127 ..... 40.3
s.3142(b) 18.2.1
(c)(1)(B) 18.2.1
s.3142(e) 18.2.1
s.3161(c)(1) 24.4.1
(h)(2) 24.4.1
s.3292 ..... 18.4.3.2, 29.11
s.3301 ..... 24.3.2
s.3486(a)(1)(A)(i)(I) 11.3
ss.3551–3586 ..... 31.2.1
s.3553(a) 31.2.1, 31.2.3, 31.2.4
(2) 31.2.1
(b) 31.2.2
(c)(2) 31.2.2
s.3561 ..... 31.2.4
s.3563(d) 31.2.4
s.3564(e) 31.2.4
s.3565(a) 31.2.4
s.3571 ..... 26.2.1, 26.7.3
(a) 31.2.3
(b)(2) 26.7.1
(3) 26.7.1, 31.2.3
(c)(2) 26.7.1
(d) 26.7.1
ss.3601–3742 ..... 31.2.1
(a)(1)(B)(i) 26.2.1
s.3664(f)(1)(A)–(B) 31.2.6
(2) 31.2.6
s.3663A(b)(4) 10.2.3
(c)(3) 24.5.1
Title 19: Customs Duties
s.1607 ..... 18.6, 31.2.5.2
Title 21: Food and Drugs
s.853 ..... 18.6
(e)(2) 18.6
(p) 18.6, 31.2.5.2
s.881(a)(4) 31.2.5.2
(7) 31.2.5.2
Title 26: Internal Revenue Code
s.6621(a)(2) 26.4
Title 28: Judiciary and Judicial Procedure
s.991–998 ..... 31.2.1
s.1332(d) 35.3.1.4
s1651(a) 26.5
s.2241 ..... 18.3.5

© Law Business Research 2021

s.2461 ..... 26.6
(c) 26.2.1
s.2462 ..... 24.3.2, 24.5.1
Title 29: Labor
s.218c 20.1
s.1132(a) 20.1
ss.2001–2009 ..... 14.4.3
s.2006(d) 14.4.3
s.2007 ..... 14.4.3
Title 30: Mineral Lands and Mining
s.815 ..... 20.1
Title 31: Money and Finance
s.3729 ..... 20.4, 20.4.2
ss.3729–3733 ..... 24.4.1
s.3730 ..... 20.4.1, 35.3.3.3
(b) 20.4, 20.4.1
(b)–(c) 20.4.1
(c)(2)(b) 20.4.1
(d) 20.4
(1) 20.4.1
(3) 20.4.1
(4) 20.4.2
(e)(4)(A) 20.4.1
(h) 20.4.2
ss.5311–5330 ..... 24.4.1
s.5318(g) 4.2.1
(k)(3)(A) 29.11
Title 33: Navigation and Navigable Waters
s.1367 ..... 20.1
Title 42: Public Health and Welfare
s.1320d2(d)(2) 41.2.2.1
s.3614(d)(1)(C) 26.3
s.5851 ..... 20.1
s.7622 ..... 20.1
s.9604(e) 11.3
Title 44: Public Printing and Documents
ss.3541–49 ..... 41.2.2.1
Title 49: Transportation
s.30171 ..... 20.1
s.31105 ..... 20.1
s.42121 ..... 20.1
Title 50: War and National Defence
s.1701 ..... 29.9
ss.1701–1702 ..... 29.9
ss.1701–1705 ..... 29.9
s.1705 ..... 26.7.3, 45.2
(a) 26.7.3, 29.9
(b) 29.9
(c) 26.7.3, 29.9

© Law Business Research 2021

Code of Federal Regulations (CFR)

Title 12: Banks and Banking
s.208 app. D–2 ..... 41.2.2.1
Title 13: Business Credit and Assistance
ss.125.8–125.10 ..... 37.1.1.1
Title 17: Commodity and Securities Exchanges
s.165.15(A)(2) 20.1.2
s.165.7(F)–(1) 20.1.2
s.200.83 ..... 35.3.1.2
s.201.600(a) 26.4
(b) 26.4
s.201.1001 ..... 26.3, 26.7.1
s.205.3(d) 6.2
s.229 ..... 41.2.2.1
s.230.405 ..... 24.5.3
s.240.21F–2 ..... 20.1.1
(b)(i) 20.1.1
s.240.21F–4(b) 20.3.1
(4)(i)–(ii) 20.3
(iii) 20.3
(7) 20.3.1
s.240.21F–6(a)(4) 20.3.1
(b)(1) 20.3
s.240.21F–7 ..... 20.3.1
s.240.21F–17 ..... 2.4.2
s.249 ..... 41.2.2.1
Title 22: Foreign Relations and Intercourse
s.1305 ..... 35.3.1.2
Title 28: Judicial Administration
s.50.9 ..... 39.1.2
Pt 80 ..... 46.4.2.3, 46.4.2.4
s.80.1 ..... 46.4.2.4
s.80.3 ..... 46.4.2.4
s.80.4 ..... 46.4.2.4
s.80.10 ..... 46.4.2.4
s.80.11 ..... 46.4.2.4
s.80.12 ..... 46.4.2.4
Title 29: Labor
s.1980.104(e) 20.1.1
(4) 20.1.1
s.1980.106 ..... 20.1.1
s.1980.107 ..... 20.1.1
s.1980.109 ..... 20.1.1
s.1980.110 ..... 20.1.1
s.1980.112 ..... 20.1.1
Pt 2570, sub pt B 24.5.3
Title 31: Money and Finance: Treasury
Pt 501 ..... 6.2, 26.7.3, 45.1.1

© Law Business Research 2021

s.501.603 45.3
s.501.701 26.7.3
Appendix A 45.1.1
(I)(I) 45.4.3.1
(III)(G) 45.4.3
Pt 510 45.1.4.3
Pt 515 (Cuba) 45.1.4.1
s.515.329 29.9, 45.2
ss.515.502–515.591 45.1.4.1
s.535.329 (Iran) 29.9
Pt 542 45.1.4.4
s.542.206 29.9
s.542.319 29.9
Pt 560 45.1.1, 45.1.4.2
s.560.215 45.2
s.560.312 26.7.3
s.560.314 26.7.3
s.560.530(3)(ii) 45.1.3
(4) 45.1.3
Pt 589 45.1.4.5, 45.4.2
Title 45: Public Welfare
Pt 160 6.6.2
Pt 164 6.6.2
ss.164.302–.318 41.2.2.1
Title 48: Federal Acquisition Regulations System
s.9.406–1(b) 26.6
(c) 26.6
s.9.406–2(a) 26.6
s.9.407–1(a) 26.6
(c) 26.6
(d) 26.6
s.9.407–2(a) 26.6

Federal Rules

Rules of Civil Procedure 18.3.2, 24.3.1, 35.3.1.2, 35.3.2.2, 39.1.4
r.11 20.4.2
r.23 35.3.1.3
(a) 35.3.1.3
r.26 37.8
(b)(1) 24.3.1, 35.4.3, 39.1.4
(3) 8.4, 37.1.2
(4) 37.8
(B) 37.8
(C) 37.8
(D) 37.8
(5)(B) 37.4.2
(c) 35.4.3
r.53 33.4
Rules of Criminal Procedure 18.3.2

© Law Business Research 2021

r.1(a)(5) 18.3.2
r.6(e) 39.1.2
r.11 16.5
r.16 37.8
(b)(1)(C) 37.8
(2)(A) 37.8
r.21(a) 39.1.2
r.26.2 37.8
(a) 37.3.1
(f) 37.8
(2) 37.3.1
r.32.2(a) 18.6, 31.2.5.2
(b)(1)(A) 18.6
Rules of Evidence 2.3.2, 18.3.2
r.408 24.3.1, 35.5.2
r.410 16.5
r.502 37.4.2
(a) 2.3.2, 37.4
(b) 37.4.2
(3) 2.3.3
(d) 37.4.2
(e) 37.4.2
r.1101(d)(3) 18.3.2

STATE LEGISLATION

Arizona

Revised Statutes Annotated
s.13–3005 40.3

California

Civil Code
Ch.5 s.1608 35.3.3.1
s.1798.81.5 41.2.2.2
s.1798.82 41.2.2.2
Code of Regulations
Title 2. Administration
s.7286.7(b) 40.3
Constitution
art. I, s.1 14.4.1
Labor Code 14.6.2.2
s.432.2 14.4.3
s.980 14.4.1, 40.3
s.2082 14.6.2.2
(a) 14.6.2.2
Penal Code
s.630 40.3
s.632(a)–(d) 14.4.2

© Law Business Research 2021

Connecticut

General Statutes Annotated
s.31–48d 14.4.2
s.52–570d 14.4.2, 40.3

Delaware

Code
Title 6: Commerce and Trade
s.17–1206 ..... 35.3.2.1
Title 8: Corporations
s.102(b)(7) 43.2.1
s.145 ..... 16.2.1, 35.3.2.3
(a) 35.3.2.3
(c) 14.6.2.2
(e) 14.6.2.2
Title 19: Labor
s.705 ..... 14.4.2
s.709A(b) 40.3
Rules of Evidence
r.502(b)(3) 2.3.3

District of Columbia

Code Annotated
s.23–542(b)(3) 40.3

Florida

Statutes Annotated
ss.934.01–934.03 ..... 14.4.2, 40.3

Illinois

Compiled Statutes Annotated
Ch.720: Criminal Offences
s.5/14–1 ..... 14.4.2, 40.3
s.5/14–2 ..... 14.4.2, 40.3
Ch.820: Employment
s.55/10 ..... 40.3
(b)(1) 40.3
2008 Biometric Information Privacy Act (740 ILCS/14 and Public Act 095-994) 40.3
s.10 ..... 40.3
s.15 ..... 40.3
s.20 ..... 40.3

Indiana

Code
art.35–33.5 (Wiretap Act) 40.3

© Law Business Research 2021

Iowa

Code
s.715C.2 ..... 41.2.2.2

Maine

Revised Annotated Statutes
Title 26: Labor and Industry
s.615 ..... 40.3

Maryland

Code Annotated
Courts and Judicial Procedure
s.10–402 ..... 14.4.2, 40.3
Labour and Employment
s.3–712(b)(1) 40.3

Massachusetts

General Laws Annotated
Ch. 93A, s.9 ..... 35.3.3.3
Ch.93H 41.2.2.2
201 CMR 17.03 ..... 41.2.2.2
Ch. 272, s.99 ..... 14.4.2, 40.3

Michigan

Comp. Laws Annotated
s.445.72 (West 2019) 41.2.2.2

Montana

Code Annotated
s.45–8–213 ..... 14.4.2, 40.3

Nevada

Revised Statutes
s.200.620 ..... 14.4.2
s.613.135 ..... 40.3

New Hampshire

Revised Annotated Statutes
Title XXIII: Labor
s.275:74 ..... 40.3
Title LVIII: Public Justice
s.570–A:1 ..... 40.3
s.570–A:2 ..... 14.4.2, 40.3
Laws Ch. 169 (H.B. 1353)(2016) 40.3

New Jersey

Revised Statutes

© Law Business Research 2021

s.2A:156A–4(d) 40.3

New York

Business Corporation Law
s.349 ..... 35.3.3.3
s.350-A 35.3.3.4
s.626 ..... 35.3.2.1
s.722 ..... 35.3.2.3
s.724 ..... 14.6.2.2
2014 Gen Bus L § 352-G (2014)
s.899–BB 41.2.2.2
Civil Service Law 20.1.3
s.75-b 20.1.3
Freedom of Information Law, N.Y. Pub. Off. Law § Ch. 47
art. 6 ..... 35.3.1.2
Labor Law
s.733 ..... 14.4.3
s.735 ..... 14.4.3
s.740 ..... 20.1.3
(2)-(3) 20.1.3
s.741(2)-(3) 20.1.3
Penal Law
s.250.00(1) 40.3
Rules of Professional Conduct
r.1.7(a)(1) 35.4.4

Ohio

Ohio Revised Annotated Code
s.2933.52(B)(4) 40.3

Oregon

Revised Statutes
s.60.394 ..... 14.6.2.2

Pennsylvania

Pennsylvania Consolidated Statutes
Title 18. Crimes and Punishments
s.5701 ..... 40.3
s.5702 ..... 14.4.2
s.5704 ..... 14.4.2

Texas

Penal Code Annotated
s.16.D2(c)(4) 40.3

Washington

Revised Code Of Washington (RCW)

© Law Business Research 2021

Title 9: Crimes and Punishment
s.9.73.030 ..... 40.3
ss.9.73.030–9.73.230 ..... 14.4.2
Title 23B: Washington Business Corporation Act
s.23B.08.520 ..... 14.6.2.2
Title 49: Labor Relations
s.49.44.200 ..... 40.3

TABLE OF OTHER NATIONAL LEGISLATION

Austria

1974 Federal Act on the Labour Constitution and Freedom of Association (BGBl. 1974/22) (Arbeitsverfassungsgesetz–ArbVG)
art.91 ..... 6.7
art.96 ..... 6.7
art.96a 6.7

France

1968 Law 68-678 (French Blocking Statute) 23.2.2.2
1980 Law 80-538 of July 16, 1980 ..... 18.5.2
1994 Penal Code 1.2.5
2016 Law No. 2016-1691, Sapin II Law 12.6

Hong Kong

Personal Data (Privacy) Ordinance (Cap 486) 6.7

Japan

2003 Act on the Protection of Personal Information (Law No. 57 of 2003) 6.7

Russia

Federal Law 'On Personal Data' (No. 152-FZ) 6.7

Switzerland

1937 Criminal Code (SR 757)
art.349 ..... 18.5.2
1991 Criminal Code (AS 2465) as amended 18.5.2

TABLE OF INTERNATIONAL TREATIES, CONVENTIONS AND AGREEMENTS

1269BC Egyptian–Hittite Peace Treaty (treaty between Egyptian Pharaoh Rameses II and Hittite ruler Hattusilis III) 32.2
1933 Extradition Treaty, Alb-US, 1 March 1933, 49 Stat. 3313 ..... 18.3.1
art.2 ..... 18.3.1
1933 Inter-American Convention on Extradition, 26 December 1933, 49 Stat. 3111 ..... 18.3.1, 32.2

© Law Business Research 2021

1950 European Convention on Human Rights and Fundamental Freedoms....1.2, 1.2.3, 1.2.4.1, 1.2.4.2, 17.3.4, 17.4.4.1, 25.10, 30.1, 32.3.5, 32.4.2, 37.3
art.1....19.2.7
art.2....38.5.1.2
art.3....17.4.4.1, 23.4, 32.3.5, 38.5.1.2
art.5....17.4.4.1
art.6....9.4.7, 9.4.8, 17.4.4.1, 32.3.5, 36.4.2, 38.5.1.1, 38.5.1.2
art.8....17.4.4.1, 19.2.7, 32.3.5, 38.5.1.2
art.10....19.2.7, 38.5.1.2
art.15....1.2.4.1
Protocol 7 art.4....1.2.4.1, 1.2.4.2
1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention)....34.6.5
art.V....34.6.5
(2)(b)....34.6.5
1959 European Convention on Mutual Legal Assistance in Criminal Matters (ETS No.030)11.5.3
1970 United Nations Convention for the Suppression of Unlawful Seizure of Aircraft, 16 December 1970, 860 U.N.T.S. 105....18.3.1
1971 Extradition Treaty, Canada-US, 3 December 1971, 27 UST 983; TIAS 8237 18.3.2, 18.3.4
art. 6....18.3.4
art. 11(1)....18.3.2
1976 Extradition Treaty, Austl-US, 8 May 1976, 27 U.S.T. 957....18.3.3
1978 Extradition Treaty, US-Germany, 20 June 1978, 32 U.S.T. 1485
art. 7(1)....18.3.1
1983 Riyadh Arab Agreement for Judicial Co-operation....32.2
Pt VI....32.2
1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988, 1582 U.N.T.S. 95....17.4.3
art. 6....18.3.1
1990 Extradition Treaty, US-Bahamas, 9 March 1990, S. Treaty Doc. 102-17, T.I.A.S. 94-922....18.3.4
art. 2(4)....18.3.4
1992 Maastricht Treaty....32.4.1
1994 Mutual Legal Assistance Treaty, US-UK, 6 January 1994, T.I.A.S. No. 96-1202
art. 19(2)....18.6
1994 Extradition Treaty, Hung-US, 1 December 1994, T.I.A.S. 97-318....18.3.4
art. 2(4)....18.3.4
1995 Extradition Treaty, Jordan-US, 28 March 1995, S. Treaty Doc. No. 104-3
art. 2(4)....18.3.4
1996 Extradition Treaty, US-Luxembourg, 1 October 1996, T.I.A.S. No. 12,804
art. 2(1)....18.3.4
1996 Extradition Treaty, US-France, 23 April 1996, S. Treaty Doc. No. 105-13; T.I.A.S. 02-201 (France Extradition Treaty)
art. 3(1)....18.3.1, 18.3.3
art. 2(4)....18.3.4
1996 Extradition Treaty, Pol-US, 10 July 1996, T.I.A.S. 99-917....18.3.1
art.4....18.3.1
1998 Extradition Treaty, Austria-US, 8 January 1998, T.I.A.S. 12916

© Law Business Research 2021

art. 2(6) 18.3.4
1998 Mutual Legal Assistance Treaty, European Union-US, 16 January 1998, T.I.A.S. 12923 ..... 18.4.3.2
1998 Extradition Treaty, S. Kor-US, 9 June 1998, T.I.A.S.12962 ..... 18.3.1
art.3 ..... 18.3.1
1998 Extradition Treaty, Para-US, 9 November 1998, T.I.A.S. 12995 ..... 18.3.1
art.3 ..... 18.3.1
2000 Extradition Treaty, Belize-US, 30 March 2000, T.I.A.S. 13089 ..... 18.3.1
art.3 ..... 18.3.1
2001 Extradition Treaty, Peru-US, 26 July 2001, T.I.A.S. 03-825 ..... 18.3.1
art.3 ..... 18.3.1
2001 Agreement on Mutual Legal Assistance in Criminal Matters between US–China 29.11
2002 Agreement on Mutual Legal Assistance in Criminal Matters between the Taipei Economic and Cultural Representative Office in the United States and the American Institute in Taiwan 29.11
2003 Extradition Treaty, US-UK, 31 March 2003, S. Treaty Doc. No. 108-23 2003, T.I.A.S. 07-426 (UK Extradition Treaty) 18.3.6, 32.2
art.2 ..... 18.3.4
(1) 18.3.4
art.3 ..... 18.3.1
art.4(1) 18.3.6
(1)–(2) 18.3.1
art.5 ..... 18.3.4
art.6 ..... 18.3.4
art.7 ..... 18.3.4
2003 Extradition Agreement, European Union-US, 25 June 2003, S. Treaty Doc. No. 109-14 18.3.1
2011 Convention on preventing and combating violence against women and domestic violence (aka Istanbul Convention) CETS No. 210 ..... 32.5.1
2016 Privacy Shield Agreement - ECJ declared the EU–US Privacy Shield invalid on 16 July 2020 ..... 18.5.2, 40.1
2019 UK–US Bilateral Data Access Agreement (Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (Washington, 3 October 2019), USA No. 6 2019) 1.3.2, 11.5.2, 12.6, 17.3.7, 18.5.2, 28.7, 40.4.2
art.2(1) 1.3.2
art.7(1) 1.3.2
2020 EU-UK agreement for implementing Brexit (Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community)
art.62(1)(l) 28.7.1, 28.7.2
art.185 ..... 28.7.2
2020 Declaration by the European Union made in accordance with the third paragraph of Article 185 of the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community 28.7.2

© Law Business Research 2021

TABLE OF EUROPEAN LEGISLATION

Treaties and Conventions

1951 Convention Relating to the Status of Refugees, (aka 1951 Refugee Convention or the Geneva Convention of 28 July 1951) 32.3.3
1957 European Convention on Extradition (ETS No.024, Paris, 13 December 1957) 17.4.2, 28.7.2, 32.2, 32.5.3
1957 Treaty of Rome
art.81 ..... 36.3.2.1
art.82 ..... 36.3.2.1
art.101 ..... 36.3.2.1
art.102 ..... 36.3.2.1
1978 Second Additional Protocol to the European Convention on Extradition (ETS No.098, 17 March 1978) 32.3.1
Ch II art.2 ..... 32.3.1
1985 Schengen Agreement 1.2.4.2
art.54 ..... 1.2.3
1990 Schengen Convention 1.2.1
art.54 ..... 1.2.1, 1.2.3
1997 Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD) 1.2.3
2000 Charter of Fundamental Rights of the European Union 1.2.5
art.50 ..... 1.2.4.2
2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/1 ..... 28.7
2001 Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [2001] OJ C 326/2 ..... 17.3.2
art.3(4) 17.3.2

Regulations

1996 Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (Blocking Statute) [1996] OJ L309/1 ..... 44.2.2, 44.2.4.1
2012 Regulation (EU) No 36/2012 of 18 January 2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011 [2012] OJ L16/1
art.29 ..... 44.5.2.1
2013 Reg.575/2013 on prudential requirements for credit institutions and investment firms [2013] OJ L 176/1 ..... 3.2.1
2014 Reg.596/2014 on market abuse (Market Abuse Regulation) [2014] OJ L 173/1 ..... 3.4.4, 19.3.4.4
art.7 ..... 2.4.6
art.17(1) 19.3.4.4
2016 Reg.2016/679 on data protection and privacy for all individuals within the European Union (General Data Protection Regulation) [2016] OJ L119/1 ..... 3.4.2, 5.6.1, 6.7, 7.7, 7.14, 11.2.4, 12.4, 18.5.2, 19.3.4.1, 19.3.4.3, 25.18, 34.6.7, 38.2.1, 38.3.1, 38.5.4, 40.1, 40.2, 40.2.1, 40.2.2, 40.2.3, 40.2.4, 40.2.5, 40.2.6, 40.2.7, 40.2.8,

© Law Business Research 2021

40.2.9, 40.3, 40.4, 40.4.1, 40.4.2, 40.2.3, 40.5, 40.6, 40.6.2, 41.2.1.2, 41.3, 41.4
Recital 32 ..... 40.2.3
art.5 ..... 7.7, 41.2.1.2
art.6 ..... 40.2.4
art.7 ..... 40.2.3
art.9 ..... 40.2.5
art.15 ..... 7.14, 40.6.2
art.28(3) 40.2.8
(a)–(h) 40.2.8
art.33 ..... 5.2, 34.6.7
art.34 ..... 34.6.7
art.48 ..... 12.4, 12.6, 40.4.2
art.49 ..... 18.5.2, 40.4.2, 40.5, 40.7
art.79 ..... 34.6.7
art.80 ..... 34.6.7
art.82 ..... 34.6.7
art.83 ..... 34.6.7
2017 Reg.2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation [2017] OJ L224/1 ..... 44.2.1
2018 Reg.2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L 26/48 ..... 41.2.1.1
2019 Law Enforcement and Security (Amendment) (EU Exit) Regulations (SI 2019/742)
Pt 14 ..... 17.4
Pt 18 ..... 17.2

Directives

1995 Dir.95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ..... 6.7
2002 Dir. 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 ..... 41.2.1.2
2014 Dir.2014/24 on public procurement and repealing Directive 2004/18/EC [2014] OJ L 94/65 ..... 23.2, 25.15
2014 Dir.2014/41 regarding the European Investigation Order in criminal matters [2014] OJ L130/1 ..... 9.9.4, 11.2.4.2, 28.7.1
2014 Dir.2014/95 as regards disclosure of non-financial and diversity information by certain large undertakings and groups [2014] OJ L330/1 ..... 19.2.7
2014 Dir.2014/104 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union [2014] OJ L 349/1 (Damages Directive) 34.7.1
2016 Dir.2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1 ..... 41.2.1.2

© Law Business Research 2021

2019 Dir.2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (EU Whistleblower Directive) [2019] OJ L 305/17 ..... 2.3.4, 19.1, 19.2.2, 40.6

Decisions

2000 Dec.2000/365 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis [2000] OJ L 131/43 ..... 1.2.3
2002 Dec.2002/584 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the EU Framework Decision [2002] OJ L 190/1 ..... 1.2.6, 17.4, 32.2, 32.4.1, 32.4.4, 32.5.2, 32.5.3
art.2(2) 32.3.1
art.4(1) 32.3.1
2003 Dec.2003/577 on the execution in the European Union of orders freezing property or evidence [2003] OJ L 196/45
art.3 ..... 17.3.7
2009 Dec.2009/948 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (Council Framework Decision) [2009] OJ L328/42 ..... 1.2.3
2016 Dec.2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) [2016] OJ L 207/1 ..... 40.2.7

© Law Business Research 2021

© Law Business Research 2021

1

Introduction to Volume I

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Celeste Koeleveld[1]

As an introduction to Volume I of the Guide, this chapter addresses UK and US law regarding two critical concepts that a company facing an investigation in either or both jurisdictions will often need to consider at the outset: corporate criminal liability and double jeopardy. This chapter also sets out in summary the priorities and challenges companies face at each stage of an investigation – topics that are explored in more detail in the chapters that follow.

Bases of corporate criminal liability 1.1

When corporate misconduct that potentially implicates multiple jurisdictions is uncovered, a critical preliminary question is: what is the test, in each jurisdiction, for corporate criminal liability? Not all countries have regimes for the criminal liability of companies, but for those jurisdictions that do, it typically rests on the premise that the acts of certain employees can be attributed to the corporation. However, the category of employees that can trigger corporate liability differs between jurisdictions – in some, it is limited to those with management responsibilities, whereas in others the category of employees who can trigger corporate liability is much broader. Generally speaking, the act triggering corporate liability must occur within the scope of the person's activities as an employee. The act must also generally be done in the interest of, or for the benefit of, the corporation. The difference between theories of liability across jurisdictions

1 Judith Seddon and Ama A Adams are partners at Ropes & Gray LLP; Eleanor Davison is a barrister at Fountain Court Chambers; Christopher J Morvillo, Luke Tolaini and Celeste Koeleveld are partners at Clifford Chance; and Michael Bowes QC is a barrister at Outer Temple Chambers.

© Law Business Research 2021

inevitably poses challenges and complicates a company's strategy for dealing with a global investigation, and in some instances can determine the outcome.

1.1.1 Corporate criminal liability in the United Kingdom

In the United Kingdom, there are two main techniques to attribute to a corporate the acts and states of mind of the individuals it employs.

The first is by use of the 'identification principle' – or identification doctrine – whereby, subject to some limited exceptions, a company may be held liable for the criminal acts of those who represent its directing mind and will, and who control what it does. The relevant test is set out in the leading case of *Tesco Ltd v. Nattrass*:[2]

> *Where a limited company is the employer difficult questions do arise in a wide variety of circumstances in deciding which of its officers or servants is to be identified with the company so that his guilt is the guilt of the company.*
>
> *I must start by considering the nature of the personality which by a fiction the law attributes to a corporation. A living person has a mind which can have knowledge or intention or be negligent and he has hands to carry out his intentions. A corporation has none of these: it must act through living persons, though not always one or the same person. Then the person who acts is not speaking or acting for the company. He is acting as the company and his mind which directs his acts is the mind of the company. There is no question of the company being vicariously liable. He is not acting as a servant, representative, agent or delegate. He is an embodiment of the company or, one could say, he hears and speaks through the persona of the company, within his appropriate sphere, and his mind is the mind of the company. If it is a guilty mind then*

2 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153; reaffirmed in *Attorney General's Reference (No. 2 of 1999)* [2000] 2 Cr App R 207 at 217–18 in which Rose LJ stated: '*Tesco v. Nattrass* is still authoritative . . . and it is impossible to find a company guilty unless its alter ego is identified. None of the authorities since *Tesco v. Nattrass* . . . supports the demise of the doctrine of identification: all are concerned with statutory construction of different substantive offences and the appropriate rule of attribution was decided having regard to the legislative intent, namely whether Parliament intended companies to be liable. There is a sound reason for a special rule of attribution in relation to statutory offences rather than common law offences, namely there is, subject to a defence of reasonable practicability, an absolute duty imposed by the statutes. The authorities on statutory offences do not bear on the common law principle in relation to manslaughter. Lord Hoffmann's speech in Meridian is a re-statement not an abandonment of existing principles'; and *Environment Agency v. St Regis Paper Co. Ltd* [2012] 1 Cr App R 177, in which, at para. 12, Moses LJ said: 'It seems to us that as a matter of statutory construction it is impossible to impose criminal liability for a breach . . . to the company in circumstances other than those where an intention to make a false entry can be attributed by operation of the rule in *Tesco Supermarkets*. There is, in our view, no warrant for imposing liability by virtue of the intentions of one who cannot be said to be the directing mind and will of [the defendant].' The identification principle was reaffirmed by the *Court of Appeal in R v. A Ltd, X, Y* [2016] EWCA Crim 1469.

© Law Business Research 2021

> *that guilt is the guilt of the company. It must be a question of law whether, once the facts have been ascertained, a person in doing particular things is to be regarded as the company or merely as the company's servant or agent.*

It is for the judge to decide, as a matter of law, whether there is evidence on which a jury could be sure that a particular individual was a 'directing mind' within the *Tesco* principles; and, if there is such evidence, the jury must then be sure that the particular individual was in fact a directing mind for the purposes of his or her particular actions. A directing mind is not necessarily limited to board directors; it may also be found in a delegate who has full discretion to act independently of instructions from the directors. In short, under the identification principle, before a corporate can be found guilty of a criminal offence, someone who represents its directing mind and will must also be found guilty. There cannot be an aggregation of acts or omissions to attribute criminal conduct to the company; rather, the criminal act or omission must be performed by a single person who can be identified with the corporate for it to be liable.

The difficulties of applying the identification principle to modern complex corporate organisations was illustrated in proceedings arising from applications to dismiss pursued by Barclays in prosecutions concerning capital raisings in 2008. The trial judge (Mr Justice Jay) and the High Court (Lord Justice Davis) held in May and November 2018 respectively that, in the circumstances of that case, where decision-making authority had been delegated to specific board subcommittees, the actions of senior executives (including the chief executive officer and chief financial officer) did not equate to the actions of the corporate organisation.[3] The Serious Fraud Office (SFO) also did not persuade either judge that any special rule of attribution should apply.[4] The SFO's attempts first to resist the application to dismiss and then to persuade the High Court to reinstate proceedings therefore failed.

The second technique of attributing liability to a company under English law is through vicarious liability. Although, in general, in the United Kingdom a corporate entity may not be convicted for the criminal acts of its inferior employees or agents, there are some exceptions, the most important of which concerns statutory offences that impose an absolute duty on the employer, even where the employer has not authorised or consented to the criminal act.[5]

---

3 The judgment of Jay J is available at https://www.judiciary.uk/wp-content/uploads/2020/02/sfo-v-barclays-dismissal-application-21-05-18.pdf. The judgment of Davis LJ is available at [2018] EWHC 3055 and https://www.judiciary.uk/wp-content/uploads/2020/02/sfo-v-barclays-judgment-12-11-18.pdf. These documents were released in early 2020 following the discontinuation of prosecutions of former Barclays executives.

4 See *Meridian Global Funds Management Asia Limited v Securities Commission* [1995] 2 AC 500.

5 These statutory offences are referred to by Rose LJ in *Attorney General's Reference (No. 2 of 1999)* [2000] 2 Cr App R 207 at 217–18, at footnote 2.

© Law Business Research 2021

Most significantly, statutory developments in the United Kingdom, starting with the offence of corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007, but more significantly the introduction of the Bribery Act 2010 and more recently Part 3 of the Criminal Finances Act 2017, represent a policy shift by introducing the offences of failure to prevent by an 'associated person' committed on behalf of the company, unless the company can demonstrate that it had adequate (or reasonable) procedures in place to prevent such offences occurring. These statutes have broad jurisdictional reach. Under the Bribery Act, for example, a corporate falling within the definition of a commercial organisation could be guilty even where no conduct occurred in, and where the associated person has no connection with, the United Kingdom.

The policy of the legislation to improve corporate governance is clear: Ministry of Justice guidance for the Bribery Act refers to the need for a corporate to create an 'anti-bribery culture'.[6] Similarly, a corporate is guilty of the offence of corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007 if the way in which its activities are managed or organised causes a person's death where a duty of care was owed. Guidance issued for the corporate offences of failure to prevent the criminal facilitation of tax evasion, which closely mirrors the Bribery Act guidance, also refers to the culture of the organisation. For example, commitment from top-level management should foster 'a culture within the relevant body in which activity intended to facilitate tax evasion is never acceptable'.[7] Each piece of legislation and accompanying guidance invites consideration of the company's culture – its attitudes, policies, systems and practices. The test for liability is closer to the test in the regulatory context where liability is based on broad principles and considers governance, and systems and controls.

It may be that this model of corporate criminal liability expands, in due course, to all economic crimes. In January 2017 the government issued a Call for Evidence (which concluded in March 2017) to examine whether the law on corporate criminal liability in the United Kingdom needs reform. It set out five options for reform, one of which was a widening of the section 7 offence. This option garnered the support of a committee of the House of Lords in March 2019 when it examined the effectiveness of the UK Bribery Act, concluding that the section 7 offence is an effective tool and calling on the UK government to expedite the decision on whether to apply the approach to other offences.[8] Since then, and in view of ongoing concerns over the

6 Ministry of Justice Guidance on the Bribery Act 2010, issued pursuant to s.9 of the UK Bribery Act 2010.

7 Her Majesty's Revenue and Customs, 'Tackling tax evasion: Government guidance for the corporate offence of failure to prevent the criminal facilitation of tax evasion', 1 September 2017, at p. 25.

8 House of Lords Bribery Act 2010 Committee, 'Bribery Act 2010 Post-legislative Scrutiny', report published 14 March 2019, https://publications.parliament.uk/pa/ld201719/ldselect/ldbribact/303/30302.htm.

© Law Business Research 2021

effectiveness of the current state of the law on corporate criminal liability, on 3 November 2020, the government asked the Law Commission to investigate the laws around corporate criminal liability and provide options to reform them. The Law Commission published its Discussion Paper in June 2021[9] and aims to publish its Options Paper in early 2022.[10] It will then work with the government on next steps, including the potential for a full Law Commission project on corporate criminal liability.[11]

In the deferred prosecution agreement (DPA) context, the current high threshold for establishing corporate criminal liability in the United Kingdom is a problem inherent in the DPA regime: to enter into a DPA, a prosecutor must satisfy the evidential test, which requires either that the evidential stage of the Full Code Test in the Code for Crown Prosecutors is satisfied,[12] or that:

> *there is at least a reasonable suspicion based upon some admissible evidence that [the company] has committed the offence, and there are reasonable grounds for believing that a continued investigation would provide further admissible evidence within a reasonable period of time, so that all the evidence together would be capable of establishing a realistic prospect of conviction in accordance with the Full Code Test.*[13]

For that reason many expected DPAs to be used principally for section 7 offences, where the identification principle does not present an obstacle to satisfying the evidential test. So too is the prospect of DPAs being used for the failure to prevent the facilitation of tax evasion offence specifically laid out in the government's guidance.[14] With all that said, three of the 12 DPAs concluded to date relate to fraud offences (*Tesco Stores Ltd*,[15] *Serco Geografix Ltd*[16] and *G4S Care & Justice Services (UK) Ltd*[17]) where both sides of the negotiation have had to grapple with the identification principle and the need for agreement on the

9 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/06/Corporate-Criminal-Liability-Discussion-Paper.pdf.

10 https://www.lawcom.gov.uk/project/corporate-criminal-liability/.

11 https://www.lawcom.gov.uk/law-commission-begins-project-on-corporate-criminal-liability/.

12 Namely that prosecutors must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction against each suspect on each charge. They must consider what the defence case may be, and how it is likely to affect the prospects of conviction. A case that does not pass the evidential stage must not proceed, no matter how serious or sensitive it may be.

13 DPA Code of Practice at para. 1.2(i)(b), https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/.

14 Her Majesty's Revenue and Customs, 'Tackling tax evasion: Government guidance for the corporate offence of failure to prevent the criminal facilitation of tax evasion', 1 September 2017, at p. 13.

15 *SFO v. Tesco Stores Ltd* [2019] Lloyd's Rep FC 283.

16 *SFO v. Serco Geografix Ltd* [2019] 7 WLUK 45.

17 *SFO v. G4S Care & Justice Services (UK) Ltd* [2020] 7 WLUK 303.

© Law Business Research 2021

existence of a 'directing mind and will'. To an extent this has also been the case in some of the DPAs concerned with bribery. Sarclad Limited,[18] in addition to section 7 culpability, also accepted primary liability in relation to conspiracies to corrupt and to bribe. Sarclad was, however, a small company and, as Sir Brian Leveson, then President of the Queen's Bench Division, found, 'there is no question but that [Sarclad] spiralled into criminality as a result of the conduct of a small number of senior executives bending to the will of agents'.[19] In other words, the identification principle did not, in that case, present a problem (although the executives who were prosecuted were all ultimately acquitted).[20] However, in *Rolls-Royce*, the DPA spanned three decades and dealt with conduct much of which pre-dated the introduction of the Bribery Act 2010 and that formed the basis of seven counts of conspiracy to corrupt and false accounting. The remaining five counts related to section 7 offences. We can conclude that in that case, despite being considerably larger than *Sarclad*, the identification principle did not present evidential hurdles in reaching a settlement. Notwithstanding this, however, in February 2019, '[f]ollowing further investigation, a detailed review of the available evidence and an assessment of the public interest', the SFO announced that there would 'be no prosecution of individuals associated with the company'.[21] Similarly, in *Amec Foster Wheeler Energy Limited*, and the two most recent DPAs with companies for Bribery Act offences,[22] the DPAs involve substantive offences of bribery (or conspiracy to commit substantive offences of bribery) as well as failure to prevent bribery contrary to section 7 of the Bribery Act 2010.[23]

The Discussion Paper recognises that 'DPAs ultimately rely on the underlying law of corporate criminal liability, and the limitations of corporate

18 Sarclad Limited was previously referred to as XYZ Limited pending the conclusion of associated proceedings against individuals. Those proceedings concluded with the acquittal of individuals in July 2019.

19 *SFO v. XYZ Ltd* (Case No. U20150856) (Preliminary Redacted) Approved Judgment, dated 8 July 2016 at para. 34.

20 https://www.sfo.gov.uk/2019/07/16/three-individuals-acquitted-as-sfo-confirms-dpa-with-sarclad/.

21 https://www.sfo.gov.uk/2019/02/22/sfo-closes-glaxosmithkline-investigation-and-investigation-into-rolls-royce-individuals.

22 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Ltd,* Crown Court (Southwark), Deferred Prosecution Agreement Judgment, 1 July 2021; *SFO v. AB Ltd and CD Ltd,* https://www.sfo.gov.uk/2021/07/20/sfo-secures-two-dpas-with-companies-for-bribery-act-offences/. In the joint cases, the DPAs only relate to the potential criminal liability of the companies and do not address whether liability of any sort attaches to any current or former employee or agent of the companies. Upon determining the issue of approval of the DPAs, the Court did not make findings of fact. No process took place by which the culpability of individual people was determined or assessed.

23 See, e.g., https://www.sfo.gov.uk/download/amec-foster-wheeler-energy-limited-deferred-prosecution-agreement-judgment-annex-3-indictment/.

© Law Business Research 2021

liability may make it harder to negotiate or enforce DPAs'. Its terms of reference[24] include, *inter alia*, consideration of whether the identification doctrine is fit for purpose, when applied to organisations of differing sizes and scales of operation; as well as considering the relationship between corporate criminal liability and other approaches to unlawful conduct by non-natural persons, including deferred prosecution agreements and civil recovery of proceeds of unlawful conduct.

Corporate criminal liability in the United States 1.1.2

The United States has long recognised principles of corporate liability based on common law and statutory bases.[25] The application of these concepts, however, has evolved over time and was most recently shaped by the global financial crisis of 2007–2008, where the spectre of industry and market collapse loomed large. Today, increasing emphasis on individual liability and corporate culture continues to shape and refine this area of law.

In the United States, the common law of agency plays an important role. Specifically, under principles of *respondeat superior*, a company may be held vicariously liable for the illegal acts of any of its agents (including employees and contract personnel) so long as those actions were within the scope of the agents' duties and were intended, even if only in part, to benefit the corporation.[26] An act is considered 'within the scope of an agent's employment' if the individual commits the act as part of his or her general line of work and with at least the partial intent to benefit the corporation.[27] The corporation need not receive an actual benefit and may be liable for these offences even if it directs its agent not to commit the offence.[28]

Moreover, even where no single employee has the requisite intent or knowledge to satisfy the *scienter* element of a crime, courts have recognised a 'collective knowledge doctrine' – where several employees collectively know enough to satisfy the intent or knowledge requirement, courts can impute this collective intent and knowledge to the corporation.[29] While historically courts have used the doctrine to establish knowledge on the part of a corporation, in recent years the doctrine has also been used to establish a corporation's intent

24 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/11/CCL-ToR-FINAL.pdf.

25 Charles Doyle, Congressional Research Service, 'Corporate Criminal Liability: An Overview of Federal Law', 1 (2013).

26 *Jones v. Federated Fin. Reserve Corp.*, 144 F.3d 961, 965 (6th Cir. 1998). See also *Hamilton v. Carell*, 243 F.3d 992, 1001 (6th Cir. 2001).

27 *United States v. Singh*, 518 F.3d 236, 249 (4th Cir. 2008) (citing *United States v. Automated Med. Labs.*, 770 F. 2d 399, 406–47 (4th Cir. 1985)).

28 *Automated Med. Labs.*, 770 F.2d at 407.

29 *United States v. Sci. Applications Int'l Corp.*, 555 F. Supp. 2d 40, 55–56 (D.C. Cir. 2008). See also *United States v. Bank of New England, N.A.*, 821 F.2d 844, 856 (1st Cir. 1987); *United States v. T.I.M.E.-D.C., Inc.*, 381 F. Supp. 730, 738–39 (W.D. Va. 1974).

© Law Business Research 2021

(i.e., to establish whether the corporation acted wilfully).[30] This doctrine is not universally accepted and some courts have limited it to circumstances where the company was flagrantly indifferent to the offences being committed.[31]

Additionally, beyond the common law principle of *respondeat superior*, some legislation imposes criminal liability for companies, including in the fields of environmental and antitrust law.[32] Such statutes have the dual effects of forcing companies to internalise the costs of their wrongdoing and of increasing the deterrent effect of the law or regulation. For example, in a field such as environmental law, where misconduct can have tremendous collateral and long-term consequences, the imposition of liability on the company acts as a strong incentive for corporate monitoring of employees and thorough due diligence and risk assessment.

Although corporate criminal liability has been a feature of US law since the nineteenth century,[33] the criminal prosecution of corporations slowed abruptly and significantly – although temporarily – following the ill-fated prosecution of Arthur Andersen in 2002; the conviction (subsequently overturned by the US Supreme Court) resulted in the firm's collapse and job losses for many thousands of innocent employees.[34] In the aftermath of the *Arthur Andersen*

30 See *United States v. Pac. Gas & Elec. Co.*, No. 14-CR-00175-TEH, 2015 WL 9460313 (N.D. Cal. 23 December 2015). There, a grand jury charged the Pacific Gas & Electric Company with violating the Pipeline Safety Act after a gas line erupted causing several deaths and injuries. The company moved to dismiss on the basis that the grand jury received incorrect instructions on, *inter alia*, collective intent. In denying the motion to dismiss, the court held that the collective knowledge of the corporation's employees demonstrated that they wilfully disregarded their legal duty to abide by the safety standards outlined in the Act. Id. at *3. Following a jury conviction on five counts, the company sought to have the case set aside; however, the court held that a reasonable juror could have found wilfulness beyond a reasonable doubt based on the evidence presented. *United States v. Pac. Gas & Elec. Co.*, No. 14-CR-00175-TEH, 2016 WL 6804575, at *3 (N.D. Cal. 17 November 2016). See also *United States v. FedEx Corp.*, 2016 U.S. Dist LEXIS 52438 (N.D. Cal. 18 April 2016) (denying FedEx's motion to dismiss, which was premised on the ground that the jury received incorrect instructions on collective intent and collective knowledge).

31 *T.I.M.E.-D.C., Inc.*, 381 F. Supp. at 740.

32 See, e.g., *United States v. Hopkins*, 53 F.3d 533 (2d Cir. 1995) (imposing a strict liability standard for a violation of the Clean Water Act); *United States v. Weitzenhoff*, 35 F.3d 1275 (9th Cir. 1993). *Contra United States v. Ahmad*, 101 F.3d 386 (5th Cir. 1996) (suggesting that there is a *mens rea* requirement for violations of the Clean Water Act). See also James Swann and Alex Ruoff, 'Self-Referral Law Seen as Barrier to New Provider Agreements', Bloomberg BNA (5 May 2016), http://www.bna.com/selfreferral-law-seen-n57982070764/ (discussing the physician self-referral law's imposition of strict liability).

33 For a discussion of the history and development of corporate criminal liability in the United States, see Kathleen F Brickey, 'Corporate Criminal Accountability: A Brief History and an Observation', 60 *Wash. U. L.Q.* 393, 404–15 (1982).

34 *Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). For a complete history of Arthur Andersen LLP, see Susan E Squires et al., *Inside Arthur Andersen: Shifting Values,*

© Law Business Research 2021

case, prosecutors became far more hesitant to unleash the brute force of criminal charges against companies.[35] Although limited prosecutions continued following *Arthur Andersen*, they were further reduced in number when, in the wake of the financial meltdown of 2007–2008, many feared that prosecuting big banks and large employers might lead to further economic turmoil.[36] This idea, that an entity might be 'too big to fail', is now widely rejected by both prosecutors and the public, and there has since been a marked uptick in prosecutions. Today, prosecutors are generally less willing to accept the prospect of dire collateral consequences as justification for not pursuing criminal charges against corporations and have required guilty pleas from large corporations, previously considered 'too big to jail'. As corporations survive – and even thrive – in the wake of guilty pleas, the spectre of the *Arthur Andersen* case recedes and the rigour with which prosecutors pursue companies continues to increase.[37]

In recent years, the United States has increasingly placed emphasis on an organisation's compliance culture and internal controls. The result is that self-reporting, full acceptance of responsibility and the disclosure of all relevant facts concerning culpable individuals (regardless of seniority) now form the basis on which the government awards co-operation credit. The Department of Justice's (DOJ) Justice Manual, the Security and Exchange Commission's (SEC) Seaboard factors, US Sentencing Guidelines and the Yates Memorandum, each of which is discussed in detail in later chapters, all reflect this pronounced shift in enforcement priorities. As a recent example, in late 2017 the DOJ introduced the Corporate Enforcement Policy, which creates a rebuttable presumption that the DOJ will grant a declination to a company in regard to Foreign Corrupt Practices Act (FCPA) violations where the company satisfies the requirements for voluntary self-disclosure, co-operation and remediation. The DOJ has also announced that it will use the Corporate Enforcement Policy as non-binding guidance in criminal cases outside the FCPA context.

Although the price of attaining corporate co-operation credit is often painfully high, most companies have no choice but to tolerate it; co-operation typically provides the best prospect for a company to prevent a criminal charge, minimise financial penalties and avoid other harsh collateral consequences,

Unexpected Consequences (2003).

35 See Gabriel Markoff, 'Arthur Andersen and the Myth of the Corporate Death Penalty: Corporate Criminal Convictions in the Twenty-First Century', 15 *U. Pa. J. Bus. L.* 797, 805–07 (2013).

36 See Gretchen Morgenson and Louise Story, 'Behind the Gentler Approach to Banks by US', *N. Y. Times*, 7 July 2011, at A1.

37 See, e.g., Peter J Henning, 'Seeking Guilty Pleas From Corporations While Limiting the Fallout', *N. Y. Times Dealbook* (5 May 2014), https://dealbook.nytimes.com/2014/05/05/seeking-guilty-pleas-from-corporations-while-limiting-the-fallout/; Francine McKenna, 'Why the Ghost of Arthur Andersen No Longer Haunts Corporate Criminals', MarketWatch (21 May 2015), https://www.marketwatch.com/story/why-the-ghost-of-arthur-andersen-no-longer-haunts-corporate-criminals-2015-05-21.

© Law Business Research 2021

such as the imposition of a monitor. Still, co-operation is not for the faint of heart, and any company operating in the United States or subject to US jurisdiction should carefully consider the far-reaching consequences – both good and bad – of setting off down the often treacherous path of co-operation. Once a company voluntarily discloses misconduct to the government, the ability to defend the case and control the process is effectively relinquished, and a company will find it very difficult to withhold sensitive, embarrassing or even harmful information. Given the highly uncertain alternative to co-operation, however, most companies accept and embrace this new reality from the start of an internal investigation and understand that factual findings far more often than not – if they involve potential criminal misconduct – will be presented to law enforcement.[38]

1.2 Double jeopardy

Another key question in any global investigation – where misconduct crosses borders and where more than one enforcement authority may seek to assert jurisdiction – is the extent to which different authorities can sanction the same or similar conduct. While domestic constitutional provisions on double jeopardy are similar between nation states, no universally accepted international norm exists, and the protection afforded by the laws in one country may offer no protection in another. This can present a major difficulty to achieving a satisfactory global settlement for a client.

The doctrine of double jeopardy is that a person should not be tried twice for the same offence.[39] Its underlying objective is to bring finality to criminal proceedings against individuals and companies in specific circumstances. Double jeopardy applies to criminal proceedings, but has been held by the European Court of Human Rights (ECtHR) to encompass an administrative penalty, in circumstances where that penalty was classified as a criminal penalty because of the nature of the charges and the severity of the punishment.[40]

In the United Kingdom, there are two essential conditions for the doctrine to apply. First, the case must be 'finally disposed of' and second, any penalty imposed must actually have been enforced or be in the process of being enforced. The rationale for the doctrine is that it confers protection on the person (individual or corporate) from the risk of repeated prosecution by the State with its greater resources.[41] Reflecting similar concerns, the concept of

38 U.S. Dep't of Justice (DOJ), Justice Manual § 9-28.700 (2015).

39 The *ne bis in idem* or double jeopardy principle is well established both in EU law and under the European Convention on Human Rights. The phrase is derived from the Roman law maxim *nemo debet bis vexari pro una et eadem causa* (a man shall not be twice vexed [or tried] for the same cause).

40 *Grande Stevens and Others v. Italy* (4 March 2014) Application Nos. 18640/10, 18647/10, 18668/10 and 18698/10.

41 The protection is not absolute. A second trial is permitted in defined circumstances. In the United Kingdom, a prosecutor will seek a retrial if a jury has been unable to reach a verdict in

© Law Business Research 2021

double jeopardy in the United States is rooted in the Fifth Amendment to the US Constitution, which reads in the relevant part: 'nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb'.[42] These 20 words have generated tens – if not hundreds – of thousands of pages of case law and are worthy of a treatise in themselves. Distilled to its essence, however, double jeopardy in the United States applies to prohibit subsequent prosecution or multiple punishments of an individual or corporation for the same conduct.[43] Nevertheless, the doctrine of double jeopardy is complicated by the question of dual sovereignty, which holds that double jeopardy's bar against successive prosecution for the same conduct does not apply when the prior prosecution was brought by a separate sovereign, for example, the US government is not barred from bringing a case where a state or another country has already prosecuted the defendant for the same conduct.

Double jeopardy in the United Kingdom 1.2.1

In England, the principle of double jeopardy is well established and has its origins in 12th-century common and ecclesiastical law. The modern principle of double jeopardy in English law was set out by the Divisional Court in *Fofana v. Deputy Prosecutor Thubin, Tribunal de Grande Instance de Meaux, France*:

> *The authorities establish two circumstances in English law that offend the principle of double jeopardy:*
> *(1) Following an acquittal or conviction for an offence, which is the same in fact and law* – autrefois acquit *or* convict*; and*
> *(2) following a trial for any offence which was founded on 'the same or substantially the same facts', where the court would normally consider it right to stay the prosecution as an abuse of process and/or unless the prosecution can show 'special circumstances' why another trial should take place.*[44]

The Divisional Court referred expressly to the United Kingdom's adoption of Article 54 of the Schengen Convention and its underlying rationale.[45] This is particularly important, as Article 54 states that a person (or company) whose case has been 'finally disposed of' by one Contracting Party may not be

---

the initial trial. A further trial in murder cases may also be permitted in circumstances where compelling new evidence comes to light.

42 U.S. Const. amend. V.

43 See generally Ernest H Schopler, Annotation, Supreme Court's Views of Fifth Amendment's Double Jeopardy Clause Pertinent to or Applied in Federal Criminal Cases, 50 L. Ed. 2d 830 (2012).

44 [2006] EWHC 744 (Admin), Judgment at para. 18.

45 Id. at para. 14.

© Law Business Research 2021

prosecuted by another for the 'same acts', provided that any penalty imposed has been enforced or is being enforced.[46]

Throughout the judgment, the Court stressed the need to look at the underlying acts behind each charge, rather than the label of the charge itself. In the event, the Court stayed the extradition proceedings on the basis that, although the extradition offence specified in the warrant was not based exactly, or solely, on the same facts as those charged in the UK indictment, there was such significant overlap between them as to require the proceedings to be stayed.[47]

In the case of *DePuy International Limited*,[48] the SFO applied the double jeopardy principle and confirmed that it will likely arise where there is or has been an investigation into the defendant's conduct by another authority overseas and the essence of a criminal offence in England and Wales is the same offence for which the defendant already faces trial, or has been acquitted or convicted. DePuy was a UK subsidiary of Johnson & Johnson, a US company that self-reported to the DOJ and the SEC bribery of foreign officials by DePuy, as well as other offences that did not involve the company, under the FCPA. Johnson & Johnson agreed to a DPA with the DOJ covering the FCPA violations and a civil sanction with the SEC that encompassed criminal and civil fines amounting to US$70 million.

The DOJ informed the SFO of the criminal conduct and the SFO commenced an investigation into DePuy and Mr Dougall, the company's marketing manager. The SFO took the view that the DPA agreed by the parent company with the DOJ had the legal character of a formally concluded prosecution that punished the same conduct that had formed the basis of the SFO investigation. It determined that the rule against double jeopardy prevented any further criminal sanction being applied in the United Kingdom and instead pursued the company using a civil route to obtain the proceeds of crime. The civil sum obtained by the SFO took into account the global settlement in the United States, including the civil fines paid and recovered of £4.8 million.

Whether a DPA under the United Kingdom's regime would qualify for double jeopardy protection remains an open question. Although entry into a DPA does not constitute a criminal conviction, it does become the final disposal of specific intended criminal proceedings on its expiry and is almost certain to include the enforcement of a fine against the corporate subject. Furthermore, prosecution may follow in the event of a breach of the DPA.

---

46 In the United Kingdom, the decision to leave the European Union adds further uncertainty to recognition of the double jeopardy principle in its application to convictions in EU Member States.

47 [2006] EWHC 744 (Admin) Judgment at para. 29.

48 SFO, Press Release, DePuy International Limited ordered to pay £4.829 million in Civil Recovery Order, 8 April 2011, available at https://webarchive.nationalarchives.gov.uk/20141106120520/http://cymraeg.sfo.gov.uk/press-room/press-release-archive/press-releases-2011/depuy-international-limited-ordered-to-pay-4829-million-in-civil-recovery-order.aspx.

© Law Business Research 2021

The *DePuy* case developed further in July 2019 with proceedings being brought in Greece against three UK nationals, Michael Dormer, Johnson & Johnson's former company group chairman, Gary Fitzpatrick, former vice president for finance at DePuy, and John Coppack, DePuy's former company secretary, as well as a number of Greek nationals. The three UK nationals were convicted of fraud and money laundering offences and sentenced to seven years in prison. As at the date of publication, these sentences are under appeal.

In addition to the convictions, the court acquitted six defendants of the charges, including DePuy's former legal director, Irene Kyriakides, and its former vice president, Robert John Dougall. Dougall was acquitted of the charges on double jeopardy grounds having already been convicted of taking part in the same bribery scheme in the United Kingdom in 2010. Some of the evidence Greek prosecutors sought to rely on to build a case against Dougall had come from the SFO following Dougall's co-operation under a section 73 Serious Organised Crime and Police Act 2005 agreement. At the Greek trial, the SFO's associate general counsel, Raymond Emson, testified to say that the agency had not consented to the use of its evidence to prosecute Dougall in Greece and that its continued use could harm UK public interest.[49]

Double jeopardy in the United States 1.2.2

As noted above, the Fifth Amendment to the US Constitution contains a double jeopardy clause. Generally speaking, the double jeopardy clause prohibits the US federal government, or any individual state, from twice prosecuting someone for the same conduct if that person has already been acquitted or convicted (or after certain mistrials once a jury has been empanelled and 'jeopardy has attached').[50] It also prohibits courts from imposing multiple punishments for the same conduct, which may be covered in multiple charges in an indictment.[51] The double jeopardy clause of the Fifth Amendment – unlike its privilege against self-incrimination – applies to both individuals and corporations.[52]

The US Supreme Court, however, has long recognised a significant exception to the double jeopardy clause, known as the 'dual sovereignty' doctrine. Pursuant to this, double jeopardy does not prohibit the federal government from prosecuting a person previously convicted or acquitted by a state, or *vice versa*, or one state from prosecuting a person convicted or acquitted by

49 https://globalinvestigationsreview.com/article/1195671/greece-convicts-three-uk-nationals-in-johnson-johnson-bribery-case#.Xa3IneLu1GM.mailto and https://globalinvestigationsreview.com/article/1195718/former-johnson-johnson-execs-to-appeal-against-greek-bribery-convictions#.Xa3JQi_97kI.mailto.

50 See *U.S. Const. amend. V; Martinez v. Illinois*, 134 S. Ct. 2070, 2074.

51 See *Breed v. Jones*, 421 U.S. 519, 528 (1975).

52 See *United States v. Martin Linen Supply Co.*, 430 U.S. 564 (1977) (applying double jeopardy to corporate defendants without discussing their status as corporations); *United States v. Sec. Nat'l Bank*, 546 F.2d 492, 494 (2d Cir. 1976).

© Law Business Research 2021

another.[53] In other words, under this doctrine the US federal government can prosecute individuals and entities for the exact same conduct that they have previously been tried for in one of the states, regardless of whether they were convicted or acquitted in that prior case.[54]

In 2019, the Supreme Court, in *Gamble v. United States*, once again reaffirmed the dual sovereignty doctrine in upholding successive prosecutions of an individual by the state of Alabama and then by the United States for the same essential conduct.[55] Although *Gamble* involved purely US domestic conduct, the Court highlighted that the dual sovereignty doctrine helped ensure the United States retained authority to prosecute extraterritorial conduct – regardless of a foreign prosecution – to vindicate US interests. In arriving at this conclusion, the Court observed:

> *There are other reasons not to offload all prosecutions for crimes involving Americans abroad. We may lack confidence in the competence or honesty of the other country's legal system. Less cynically, we may think that special protection for US nationals serves key national interests related to security, trade, commerce, or scholarship. Such interests might also give us a stake in punishing crimes committed* by *US nationals abroad – especially crimes that might do harm to our national security or foreign relations.*[56]

The Court's cynicism aside, this decision clearly underscores the prudence of pre-resolution engagement with US authorities for companies and individuals facing investigations in a foreign jurisdiction where US interests might be implicated.

Nevertheless, while the law clearly allows successive prosecutions in such instances, to blunt the potentially harsh impact of the dual sovereignty exception, the DOJ has adopted a policy that precludes the initiation of federal prosecution following a prior state (or federal) prosecution based on substantially

53 *Gamble v. United States*, 139 S. Ct. 1960 (2019). See also, *United States v. Lanza*, 260 U.S. 377, 385 (1922).

54 Notably, the Supreme Court very recently declined to extend the dual sovereignty doctrine to successive prosecutions by Puerto Rico and the United States, concluding that the question of separate sovereignty requires an assessment of the source of the power to punish. *Puerto Rico v. Sanchez Valle*, 136 S. Ct. 1863 (2016). There, the Court held that successive prosecutions may be brought only where two prosecuting authorities derive their power to punish from independent sources; if those authorities draw their power from the same ultimate source, successive prosecutions are prohibited.

55 *Gamble*, 139 S. Ct. at 1964.

56 Id. at 1967 (emphasis in original).

© Law Business Research 2021

the same facts. The Dual and Successive Prosecution Policy (the Petite Policy) seeks:

> *to vindicate substantial federal interests through appropriate federal prosecutions, to protect persons charged with criminal conduct from the burdens associated with multiple prosecutions and punishments for substantially the same act(s) or transaction(s), to promote efficient utilization of Department resources, and to promote coordination and cooperation between federal and state prosecutors.*[57]

To overcome this policy, federal prosecutors must not only comply with the standards applicable for commencing any federal prosecution (i.e., that the defendant's conduct constitutes a federal offence and that the admissible evidence probably will be sufficient to obtain and sustain a conviction by an unbiased trier of fact), but they must also obtain the approval of the appropriate Assistant Attorney General and establish that (1) the matter involves a substantial federal interest; and (2) the prior prosecution left that federal interest 'demonstrably unvindicated'. It is the second of these two factors that provides the greatest protection against successive prosecutions, as, under this policy, the DOJ 'will presume that a prior prosecution, regardless of result, has vindicated the relevant federal interest'.[58] While this presumption can, of course, be overcome (and the policy lists the factors relevant to make such an assessment),[59] federal prosecutors traditionally reserve such challenges for those cases where it perceives the preceding result to have been manifestly unjust.

Notably, the Petite Policy does not expressly preclude the DOJ from bringing criminal charges based on the same conduct previously prosecuted by a foreign sovereign. Nevertheless, similar, if not identical, principles are at play whether the prior prosecution was brought by a state or federal government, or a foreign sovereign. Counsel endeavouring to persuade the DOJ to defer to the foreign result certainly should be prepared to demonstrate why a successive prosecution would contravene that policy. The DOJ will, of course, consider if US interests have been sufficiently redressed by the foreign prosecution.[60] And, in the cases of corporate criminal activity, it is likely that the DOJ will seek to exact a penalty based on the harm to its interests.

Still, if a prior prosecution by a foreign sovereign has resulted in adequate penalties proportionate to the conduct, the DOJ may well decline or defer the prosecution or, perhaps, offset any US fines or penalties by the amounts paid

57 DOJ, Justice Manual § 9-2.031 (1999).

58 Id.

59 Id.

60 See *Thompson v. United States*, 444 U.S. 248, 248 (1980) (noting that there is an exception to the Petite Policy where US prosecution would serve 'compelling interests of federal law enforcement').

© Law Business Research 2021

abroad, particularly in the corporate context. This is particularly likely in the wake of the DOJ's new policy, announced in May 2018 and since incorporated into the DOJ's Justice Manual, to discourage the 'piling on' of multiple penalties by the DOJ and foreign and domestic agencies when they are investigating the same corporate misconduct.[61] The policy articulates certain factors to be used when determining whether the imposition of multiple penalties would nevertheless serve the interest of justice, and therefore there is no certainty that prior prosecution by a foreign sovereign will result in no or lenient punishment by the United States.

The double jeopardy clause generally does not restrict the ability of the US government to pursue successive criminal and administrative remedies for the same conduct.[62] Indeed, while it is more common for administrative investigations to run in parallel with DOJ investigations, double jeopardy is not offended when a criminal prosecution follows the imposition of an administrative sanction (or *vice versa*). As the Supreme Court held in *Hudson v. United States*, the double jeopardy clause does not apply to non-criminal penalties.[63] Though the Court in *Hudson* recognised that criminal charges following in the wake of stinging administrative penalties could potentially implicate double jeopardy concerns, a defendant mounting such a challenge must establish by the 'clearest proof' that the administrative penalty was so punitive as to render it criminal for double jeopardy purposes – a very high hurdle indeed.[64]

1.2.3 The application of double jeopardy in the EU and under the ECHR

Increased focus on combating overseas corruption following the signing of the Organisation for Economic Co-operation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions has resulted in a rise in multiple prosecutions. A person or company engaging in overseas corruption faces the prospect of prosecution in any signatory country where he, she or the company may have sufficient involvement, either by citizenship or place of incorporation, or as a place where relevant acts took place.

The picture is evolving on both the supranational and national levels, and this is discussed below. The double jeopardy principle is set out in Article 54 of the 1985 Schengen Agreement.[65] On 29 May 2000, the United Kingdom adopted Article 54 of the Schengen Convention and so it presently forms part

61 DOJ, Justice Manual § 1-12.100; Deputy Att'y Gen. Rod Rosenstein, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

62 See *Hudson v. United States*, 522 U.S. 93, 96 (1997).

63 Id. at 99.

64 See id.

65 Article 54: 'A person whose trial has been finally disposed of in one contracting party may not be prosecuted in another contracting party for the same acts provided that, if a penalty has

© Law Business Research 2021

of the domestic law.[66] The rationale for the application of the principle across the European Union was made clear in *R v. Gozutok and Brugge*,[67] as permitting finality in criminal proceedings and also engendering mutual trust in national criminal justice systems by requiring that each Member State recognise the criminal laws in force in the others even when the outcome would be different if its own national law had been applied.

The Council Framework Decision 2009 on the prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (the EU Framework Decision)[68] sets out measures to prevent situations where the same person is subject to parallel criminal proceedings in different Member States in respect of the same facts that might lead to the final disposal of those proceedings in two or more Member States.

Since the end of the transition period, the EU Framework Decision is no longer binding on the United Kingdom, and therefore need not be taken into account by the SFO in its decision whether to open a criminal investigation. However all the indications from the SFO are that they will continue to coordinate closely with the EU Member States.[69] The double jeopardy principle is not a bar to a criminal investigation, however, and the SFO has very wide discretion in deciding whether to carry out an investigation.[70]

European human rights jurisprudence 1.2.4

European Court of Human Rights 1.2.4.1

Article 4 of Protocol 7 to the European Convention on Human Rights (ECHR) specifically recognises the double jeopardy principle.[71]

---

been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing contracting party.'

66 2000/365/EC: Council Decision of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis.

67 [2003] 2 CMLR 2.

68 2009/948/JHA.

69 See, for example, https://www.sfo.gov.uk/2020/10/09/future-challenges-in-economic-crime-a-view-from-the-sfo/.

70 Section 1(3) of the Criminal Justice Act 1987: 'The Director may investigate any suspected offence which appears to him on reasonable grounds to involve serious or complex fraud.' See also *R (Corner House) v. Director of the SFO* [2008] EWHC 714 (Admin) at para. 51.

71 *Article 4 – Right not to be tried or punished twice*

1 No one shall be liable to be tried or punished again in criminal proceedings under the jurisdiction of the same State for an offence for which he has already been finally acquitted or convicted in accordance with the law and penal procedure of that State.

2 The provisions of the preceding paragraph shall not prevent the reopening of the case in accordance with the law and penal procedure of the State concerned, if there is evidence of new or newly discovered facts, or if there has been a fundamental defect in the previous proceedings, which could affect the outcome of the case.

3 No derogation from this Article shall be made under Article 15 of the Convention.

© Law Business Research 2021

The importance of the principle was emphasised in the European Court of Human Rights' (ECtHR) Chamber judgment in the case of *Grande Stevens and Others v. Italy*.[72] Here, the applicants received an administrative penalty from Consob, the Italian Companies and Stock Exchange Commission, in respect of providing false or misleading information concerning financial instruments. The penalty took the form of substantial fines and various banning orders. Subsequently, the applicants were committed for trial before the Turin District Court in respect of criminal allegations of market abuse arising out of the same facts.

The applicants argued before the ECtHR that the subsequent criminal proceedings were in breach of Article 4 as the applicants had already been subject to a penalty that was akin to a criminal penalty, even though it was imposed in an administrative context. The court accepted their argument and ruled that the administrative penalty should be considered a criminal penalty for the purposes of the ECHR and that Article 4 prevented the criminal proceedings from taking place on the grounds of double jeopardy.[73]

1.2.4.2 Court of Justice of the European Union

Three further cases arose in Italy in 2008, in which the principle of double jeopardy was considered, again in relation to administrative penalties imposed by Consob which were severe enough to be considered criminal in nature. All these cases were referred to the Court of Justice of the European Union (CJEU) by Italy's Supreme Court of Cassation for a preliminary ruling considering Article 50 of the Charter of Fundamental Rights of the European Union and Article 4, Protocol 7 ECHR.

In the *Ricucci* matter,[74] the defendant had been fined €10.2 million by Consob, as well as being convicted in criminal proceedings resulting in a sentence of four years' imprisonment for alleged market manipulation. The Rome District Court subsequently pardoned Ricucci in a final judgment.

Ricucci challenged Consob's fine in Rome's Court of Appeal, which reduced it to €5 million in 2009. He then took his appeal to Italy's Supreme Court of Cassation, where he argued that his 2008 criminal conviction and subsequent pardon should negate any Consob proceedings. The Court of Appeal asked the CJEU whether the *ne bis in idem* principle in Article 50 gives individuals

72 *Grande Stevens and Others v. Italy* (4 March 2014) Application Nos. 18640/10, 18647/10, 18668/10 and 18698/10.

73 In March 2015, France's Constitutional Court ruled that Airbus executives could not be prosecuted for insider trading because they had been cleared over similar administrative charges by France's Financial Markets Authority, the AMF. In reaching its decision, the Court gave considerable weight to the decision of the ECtHR in the *Grande Stevens* case.

74 Case C-537/16: Judgment of the Court (Grand Chamber) of 20 March 2018 (request for a preliminary ruling from the Supreme Court of Cassation – Italy). See also https://globalinvestigationsreview.com/article/1168169/cjeu-italian-defendants-should-not-face-double-jeopardy.

© Law Business Research 2021

a direct right that can be applied to negate dual proceedings. The Court also asked the CJEU whether the *ne bis in idem* principle precludes Italy's law allowing administrative proceedings to be brought for market manipulation after a defendant has been finally convicted.

The CJEU held that dual proceedings can be pursued if they meet 'an objective of general interest' – in this case, to protect the European Union's financial interests. However, the national legislation must also ensure that proceedings and the severity of penalties are limited to 'what is strictly necessary' where dual proceedings are to be pursued. Italy's market manipulation law did not respect the principle of proportionality, and the CJEU ruled that, if a criminal penalty already punishes misconduct in an 'effective, proportionate and dissuasive manner', administrative proceedings of a criminal nature are gratuitous and so go beyond 'what is strictly necessary'.

In two other cases, *Di Puma* and *Zecca*,[75] appeals were made against Consob fines, with the defendants arguing that they should not face administrative charges for insider trading when a criminal court had found no misconduct. The appeals court asked the CJEU whether, in light of *ne bis in idem*, a court would violate an EU directive that requires Member States to provide 'effective, proportionate and dissuasive penalties' for insider trading if it did not bring administrative sanctions after a criminal court found no wrongdoing.

The CJEU determined in its preliminary ruling that not bringing administrative sanctions after a criminal court has found no misconduct is in accordance with EU law because of the principle of *res judicata*. It ruled that a defendant who is cleared of a criminal charge should not be the subject of administrative proceedings for the same matter.

The CJEU has considered the application of the double jeopardy principle to the Schengen Agreement in the context of an individual under investigation in Poland and Germany for allegations of extortion.[76] In this case it upheld the German prosecutor's decision that the double jeopardy principle did not apply. The matter had not been finally disposed of as no detailed investigation had taken place.

On 15 November 2016, the CJEU rejected an appeal brought by two applicants who were penalised by the Norwegian Tax Authority for failing to pay tax in 2008 and then convicted of aggravated tax fraud in 2009 by the National Authority for Investigation and Prosecution of Economic Crime. The applicants claimed they were being prosecuted twice for the same misconduct in violation of double jeopardy rules. Rejecting the application, the court held that ECHR double jeopardy rules are not violated where the contracting party could satisfy the court that dual proceedings are sufficiently connected in time and space so as to represent a coherent whole, rather than two sets of proceedings.[77]

75 Joined Cases C-596/16 and C-597/16, *Di Puma and Zecca*.

76 Case C-486/14, *Kossowski*, 29 June 2016.

77 *Case of A and B v. Norway* (Applications nos. 24130/11 and 29758/11), 15 November 2016, lovdata.no/static/EMDN/emd-2011-024130.pdf.

© Law Business Research 2021

1.2.5 Double jeopardy in France

Recent developments in France continue to warrant a special mention as the issue of double jeopardy and its application has come before the courts on a number of occasions in recent years. The appellate courts have considered the extent to which domestic law will recognise convictions in the United States as a bar to prosecution, as well as the status of US DPAs in domestic proceedings. On 18 June 2015, a criminal court in Paris acquitted four French companies that were accused of paying bribes in connection with the United Nations' Oil-For-Food Programme on the grounds that they (or their corporate parents) had already signed DPAs with the DOJ. The rationale given was that it was inconsistent with French international obligations to prosecute the companies for a second time on what the Court found to be the same facts. The prosecutor's appeal against the acquittal was successful and in February 2016 a Paris court fined Total SA €750,000 for corrupting foreign officials.

Separate criminal proceedings were successfully pursued in France against Total for corruption of a foreign public agent (a senior energy official in Iran) resulting in a €500,000 fine being imposed in December 2018. The prosecution unsuccessfully sought confiscation €250,000 it had argued were the proceeds of the corruption. In relation to the same matters, Total entered into a US$245.2 million, three-year DPA with the DOJ and disgorged US$153 million in an SEC cease-and-desist order. The DPA expired in November 2016.

On 26 February 2018, the Court of Cassation in Paris upheld a decision to fine Swiss energy company Vitol €300,000 for making corrupt payments to the Iraq government as part of the United Nations Oil-For-Food programme.[78] The Court rejected Vitol's argument that it was protected from criminal proceedings in France because it had already been punished in the United States. The Court found that double jeopardy did not apply because the company had pleaded guilty to a different charge in US proceedings[79] and stated that France must maintain its right to punish companies that break French law. In its ruling, the Court of Cassation considered double jeopardy protections enshrined in both France's Penal Code and the Charter of Fundamental Rights of the European Union. It concluded that both those protections fail to immunise a company from being prosecuted twice if part of the offence occurred within France and if the misconduct is prosecuted by a country that is not bound by French or EU

78 The fine was in addition to a US$17.5 million sanction Vitol received in the United States in 2007 as part of a plea agreement entered to resolve identical allegations.

79 The company pleaded guilty to a single count of grand larceny in the New York State Supreme Court and paid a US$17.5 million fine, US$4.5 million of which was donated to the state of New York. Vitol admitted in the US plea deal that corrupt payments were made through its employees in France. In total, the company said it paid US$13 million to Iraqi officials between 2001 and 2002 hidden in oil contracts awarded to the company as part of the Oil-For-Food programme.

© Law Business Research 2021

law, such as the United States.[80] This significantly weakens the double jeopardy defence, in circumstances where some of the misconduct occurred in France.

These cases demonstrate the potential unfairness to a corporate that has effectively admitted the offence in another jurisdiction to obtain a DPA and then finds those admissions being used against it in a jurisdiction that does not recognise the DPA under the double jeopardy doctrine.

Conclusion 1.2.6

At first sight, the doctrine of double jeopardy appears to be a substantial protection against repeated prosecution in respect of the same conduct. However, although the doctrine may in some circumstances protect against a similar prosecution within the state, or member group such as the European Union, it may well fail to protect against a prosecution brought by a separate state. France's decision not to apply the principle in circumstances where part of the offence occurred within its sovereign territory is a significant restriction on its scope.

As many countries do not recognise a foreign conviction for the purposes of double jeopardy, it is not possible to reassure a corporate client that a criminal settlement in one jurisdiction will qualify as a settlement in others as well. Further, entering into a DPA in one jurisdiction may risk damaging the client's interests in another if the DPA is not recognised as a bar to prosecution, but the admissions it made to secure the DPA are admissible against it in other jurisdictions.

The picture is uncertain and many questions remain unanswered. These include:

- Should there be international recognition of criminal convictions for the purposes of double jeopardy, to encourage global settlements?
- Should DPAs be given the status of a criminal conviction for the purposes of double jeopardy?
- Should regulatory sanctions qualify for the purposes of double jeopardy?

Until these issues are resolved, a corporate client will only be able to place very limited reliance on the double jeopardy principle as a bar to further prosecution in respect of the same conduct. At present, the only safe course will be to seek to negotiate a global settlement with all the states most likely to take an interest in the conduct, before admitting guilt in any state. Whether this is practicable will vary from case to case.

In relation to individuals, an issue of note was recently referred to the CJEU stemming from a dispute between Hungary and Croatia in the case of *AY*.[81]

80 Note that as France is a civil law jurisdiction, lower courts are not strictly bound to follow the Court of Cassation's decision.

81 Judgment in Case C-268/17 *AY (Arrest warrant – witness)*. The Court analysed whether any of the grounds for optional non-execution provided for in Article 4(3) of the framework decision applied in the *AY* case and concluded they did not. Those grounds relate to (1) the decision of the executing judicial authority not to prosecute for the offence on which the European arrest

© Law Business Research 2021

The Croatian court had sought a preliminary ruling on whether the double jeopardy principle under EU law means Member States may refuse to enforce European arrest warrant (EAW) requests in cases where its investigations treated individuals as witnesses and not suspects. Specifically, Croatia asked whether Hungary could refuse to enforce two EAW requests it issued for an individual, named only as AY, to prevent damage to reputation, after AY was treated as a witness rather than a suspect in an investigation conducted by the Hungarian prosecutor's office. In its judgment of July 2018, the CJEU stated that execution of an EAW cannot be refused on the ground that a prosecutor had closed a criminal investigation where, during that investigation, the requested person was interviewed as a witness only. The Court stated that the judicial authorities of the Member States must adopt a decision on any EAW communicated to them.

1.3 The stages of an investigation

Issues that at first glance may appear to be isolated or technical can quickly spread across borders and escalate into multifaceted threats to businesses, reputations and careers. Even within jurisdictions, different enforcement authorities operate within their own, often complex, legal and technical frameworks. Any investigation, whether an internal fact-finding inquiry aimed at establishing the size and nature of a problem or one commenced by an enforcement authority, is inevitably a dynamic process. There can be no 'one-size-fits-all' approach and the scope of an investigation can change significantly as it progresses.

Nonetheless, it is possible to identify three broad, and often overlapping, phases to an investigation, namely the commencement, information-gathering and disposal phases. Particular challenges arise, and sometimes recur, at each of these.

warrant is based, (2) the fact that, in the executing Member State, the judicial authorities have decided to halt proceedings in respect of the offence on which the warrant is based, and (3) the fact that a final judgment has been passed on the requested person in a Member State in respect of the same acts, which prevents further proceedings. The Court determined the first and third grounds were irrelevant in the case. The Court concluded that an interpretation according to which the execution of a European arrest warrant could be refused where that warrant concerns the same acts as those that have already been the subject of a previous decision, without the identity of the person against whom criminal proceedings are brought being considered relevant, would be manifestly too broad and entail a risk that the obligation to execute the warrant could be circumvented. As that ground for non-execution constitutes an exception, it must be interpreted strictly and in the light of the need to promote the prevention of crime. The investigation by the Hungarian authorities was conducted, not against AY, but against an unknown person, and the decision that closed that investigation was not taken in respect of AY. The Court concludes from this that the second ground for non-execution does not apply either. See also https://globalinvestigationsreview.com/article/1166589/croatian-case-to-clarify-eaw-double-jeopardy-rules.

© Law Business Research 2021

Conducting and handling investigations, limiting the damage they cause and bringing them to as swift and efficient a conclusion as possible is an art rather than a science. It requires advisers to anticipate, balance and respond to a wide variety of challenges, and to appreciate the potential ramifications of every interaction with a diverse cast of characters.

Commencement 1.3.1

When deciding whether or how to commence an investigation, or how best to respond to one already commenced by an enforcement authority, it is axiomatic that the very first task to be carried out must be to establish as precisely as possible the size and shape of the problem. Which corporate entities and individuals are regarded as subjects of the investigation? Which offences are they thought to have committed, and which regulatory provisions might they have infringed? Are any other local or foreign agencies investigating (or likely to investigate) this misconduct?

In some cases (typically those involving alleged breaches of regulatory requirements), the answers will be self-evident from notices from authorities confirming the commencement of an investigation or the appointment of investigators, and there may be opportunities to seek to establish more detail through scoping discussions. However, in other cases (typically those involving alleged criminal misconduct), the investigators will not necessarily provide details or opportunities for discussion. In some cases, the first indication an individual or entity receives of an investigation by an enforcement authority will be a requirement to attend an interview or provide documents, or, worse still, a knock at the door from investigating officers. In all cases – whether or not enforcement authorities are already aware of alleged misconduct – steps must be taken immediately upon discovery of the alleged misconduct to preserve and to avoid the destruction or deletion (inadvertent or otherwise) of documents that are, or could become, relevant. In large multinational organisations, identifying the custodians of these documents, drafting and disseminating appropriately inclusive document-retention notices, gathering the material and suspending automatic deletion policies is a substantial undertaking in itself.

Where authorities are not already aware of apparent misconduct, considering whether, when and how to disclose matters to them will be an immediate priority. In some cases, specific regulatory obligations will require disclosures. In others, it may be appropriate to voluntarily report matters to maximise the prospects of a consensual resolution on favourable terms. Both types of disclosures require careful handling. Consideration must be given to potential consequences, both for those individuals or corporates already implicated in alleged misconduct, and for those that may become so. Where information is disclosed voluntarily, wider considerations about whether co-operation will be appropriate and would be likely to encourage the relevant enforcement authority to curtail its investigation (and on which terms) should be borne in mind. Identifying the potential risks and benefits will typically involve assessing the enforcement policy and posture of each agency involved (and often of individual

© Law Business Research 2021

investigators) and its ability and propensity to pass information to other investigating or prosecuting authorities (both within and between jurisdictions).

These assessments will inform the answers to a number of practical questions:

- Should an initial notification be made before a full internal investigation has been undertaken?
- What should be disclosed at the end of the internal investigation and to whom?
- Should information be disclosed to the authorities orally rather than in writing?
- Will investigators regard anything less than unfettered access to witnesses' first accounts and other underlying documents as true co-operation enabling them to contemplate a negotiated outcome?
- Is it feasible to maintain claims to legal professional privilege or challenge investigators' actions or demands while still seeking to claim that the subjects of the investigation are co-operating?

Some of these questions have been addressed in chapters of the SFO Operational Handbook published during 2019 and 2020, in particular the chapter on Corporate Co-operation Guidance, published in August 2019[82] and, more recently, in the chapter on 'Deferred Prosecution Agreements' published on 23 October 2020.[83] These provide greater clarity on the circumstances in which the SFO will be prepared to commence discussions with a view to potentially concluding investigations by way of DPAs and insight into how the SFO interprets and approaches particular principles set out in the legislation and formal guidance.

Choices made at this stage about how much information and control to relinquish over the investigative process and the robustness of the line to be taken with investigators in relation to issues such as privilege can be crucial in setting the tone for the rest of the investigation, and any proceedings that flow from it. It is critical for companies, when deciding which stance to take at the commencement stage, to anticipate what enforcement authorities and courts may require at later stages and what the collateral effect of decisions about how much information to provide and how proactively to assist those authorities may be. The DPA agreed between the SFO and Sarclad illustrates this point. Following the conclusion of the DPA, former senior executives being prosecuted by the SFO sought to compel the SFO to obtain and disclose to them copies of notes of interviews relevant to the SFO's decision to enter into a DPA with the company.[84] The notes had not been previously provided to the SFO during DPA negotiations as Sarclad declined to waive privilege and the SFO

82 SFO Operational Handbook, 'Corporate Co-operation Guidance', available at https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

83 Id., 'Deferred Prosecution Agreements', available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/.

84 *R (on the application of AL) v. Serious Fraud Office* [2018] EWHC 856.

© Law Business Research 2021

agreed to proceed on the basis of summaries of the interviews prepared on the basis of 'oral proffers' delivered by Sarclad's lawyers. Although the High Court, hearing the challenge brought by the former senior executives being prosecuted (and who were subsequently acquitted in July 2019), declined to order the SFO to obtain and disclose the additional documents, it deprecated the approach taken by the SFO. As a consequence, as is confirmed in its Corporate Co-operation Guidance, the SFO is likely to take a more stringent approach when deciding which documents it requires during DPA negotiations.

In 2018, the Court of Appeal allowed ENRC's appeal against the first-instance decision, upholding its claim to litigation privilege over the disputed documents, including notes of witness interviews.[85] Under the leadership of the Director of the SFO, Lisa Osofsky, the SFO decided not to appeal that decision. Given the importance of privilege in the context of global investigations, the decision was welcomed by lawyers across the globe – the Court of Appeal's judgment aligned the law more closely with the law of privilege in the United States and its clear articulation of the applicability of litigation privilege in the context of a criminal investigation is likely to mean that the SFO will be less aggressive in making assertions that privilege claims by companies over documents created during the course of internal investigations are ill-founded than it was before the ruling. However, it is unlikely that the SFO will be any less willing to request waivers of privilege, particularly since the Court of Appeal judgment was clear that its decision should not 'impact adversely' on the deferred prosecution regime in the United Kingdom, and emphasising the relevance of waiver to an assessment of a company's co-operation in reaching resolutions.[86]

The SFO's Corporate Co-operation Guidance addresses this point but does not provide a definitive answer. It acknowledges (as is evident from the DPAs concluded to date) that declining to waive privilege is not necessarily fatal to a settlement subsequently being agreed and simply states that a company declining to waive privilege does not attain the corresponding benefit set out in the DPA Code of Practice, but will not be penalised by the SFO. The deferred prosecution agreements guidance reiterates that a company can neither be compelled to waive privilege, nor penalised for not waiving privilege. In practice, this superficially neutral stance is likely to translate into significantly more difficult discussions, both with the SFO about whether it is appropriate to commence DPA negotiations, and in due course with the SFO and the court about whether any proposed DPA should be concluded and approved. Decisions as to the approach taken by a company to privilege, regardless of

85 *SFO v. ENRC* [2018] EWCA Civ 2006.

86 See *SFO v. ENRC* [2018] EWCA Civ 2006 at paras. 115–17, in particular: 'In any event, to determine whether a DPA is in the interests of justice, and whether the terms of the particular DPA are fair, reasonable and proportionate, the court must examine the company's conduct and the extent to which it cooperated with the SFO. Such an examination will consider whether the company was willing to waive any privilege attaching to documents produced during internal investigations, so that it could share those documents with the SFO.'

© Law Business Research 2021

whether privilege can properly be asserted or not, will continue to be crucial decisions that set the tone and, possibly, direction of an investigation and any proceedings flowing from it.

In cases involving allegations made by or against directors or employees, early determinations need to be made as to whether any specific whistleblower protection legislation or rules have been engaged and whether action should be taken to suspend or dismiss those individuals, or at least limit their involvement in decision-making in relation to investigations.

1.3.2 Information gathering

Once the scope of an investigation has been determined, the process of gathering and analysing relevant information, whether in documentary or electronic form or in the form of witnesses' accounts, commences. Since the advent of the European investigation order (introduced in England and Wales in 2017), the process of gathering information across borders has been a much simpler and quicker process for enforcement authorities in Europe.[87] In October 2019, the SFO's (and other agencies') powers were further extended as new legislation came into force enabling them to apply to the court to secure access to electronic data held by communications services providers overseas (provided certain international co-operation agreements are in place in the jurisdiction concerned).[88] Following the completion of the necessary steps by the UK Department of Justice, the UK–US Bilateral Data Access Agreement[89] came into force on 8 July 2020 (subject to one proviso), enabling the SFO and other agencies more easily to seek data located in the United States. The Agreement appears to require that appropriate targeting limitations should be in place before it comes into force.[90] The framework for creating targeting and minimisation procedures is set out in Article 7. These procedures are intended to provide some safeguards for those targeted by an order made under the agreement.[91]

In substantial cross-border investigations, the task of collating relevant material, ascertaining whether it is responsive to requirements to produce documents or provide information (or whether it should otherwise be produced to demonstrate a co-operative stance), and filtering it to remove material exempt from disclosure is time- and resource-intensive. It often requires specialist technical input and expertise. Information should not be treated as a readily portable commodity, and careful consideration should be given to applicable data protection and other confidentiality constraints before information is

87 See Criminal Justice (European Investigation Order) Regulations 2017.

88 See Crime (Overseas Production Orders) Act 2019.

89 Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (Washington, 3 October 2019), USA No. 6 2019.

90 Id., Article 2, para. 1.

91 Id., Article 7, para. 1.

© Law Business Research 2021

transferred between jurisdictions during internal investigations or produced to investigating authorities.[92]

Witness interviews during internal investigations raise no fewer questions. When should interviews take place? Who should be present? What material and questions is it appropriate to put to them during such interviews? Should they be represented (and, if so, at whose expense)? Taking a wider view across all jurisdictions in which action could be taken, and from the individual's perspective, is it in the interests of subjects of the investigation to provide information voluntarily, or should they insist on being compelled to do so?

Covid-19 has brought considerable additional complexities for enforcement authorities and corporate organisations conducting investigations. In particular, investigations being conducted by the SFO are likely to be delayed by the disruption arising from the pandemic, as it has encountered difficulties making full use of technological solutions to process documentary material in electronic form, and has been more reluctant than some other UK enforcement authorities to conduct interviews remotely (particularly those involving subjects of investigations).

Of course, where investigations by the authorities have already begun, investigating authorities will be keen to interview individuals who are suspects. Depending on the nature of the investigation and the allegations against them, it may be open to individuals to remain silent in response to questions (although this course of action may limit their options in any proceedings flowing from the investigation). Conversely, it may serve such individuals' interests to proactively volunteer information to secure more lenient treatment by authorities, or ultimately the courts.

92 Recent developments in the United Kingdom and United States are relevant. In the United Kingdom, a decision by the Administrative Court in September 2018, *R (on the Application of KBR Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), which had extended section 2 notices, served in the United Kingdom, extraterritorially to foreign companies in respect of documents held outside the jurisdiction when there was a sufficient connection between the company and the jurisdiction, was overturned by the Supreme Court on 5 February 2021. In a unanimous judgment, the Court held that the SFO could not use the power in s.2(3) to require foreign companies to produce documents held outside the United Kingdom; such a broad reading was inconsistent with the intention of Parliament and should not be inferred (https://www.supremecourt.uk/cases/docs/uksc-2018-0215-judgment.pdf). In the United States, following the successful appeal by Microsoft of orders holding it in contempt for failure to comply with a warrant requiring it to produce the contents of a customer's email account stored on a server outside the United States, Congress enacted on 23 March 2018 the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), providing expressly for extraterritorial application and thereafter the United States obtained a fresh warrant against Microsoft.

© Law Business Research 2021

1.3.3 Disposal

As the information gathering progresses, and evidence is assimilated and understood, a decision will need to be reached as to whether this may be resolved through negotiation, or whether the individual or company disputes the allegations entirely or is unprepared to reach any resolution or enter into any settlement that requires admissions of misconduct.

Where settlement is an option, from economic, commercial and reputational standpoints, settling quickly with as many investigating authorities as possible, and on the most favourable terms possible, is likely to be preferable. Particularly in regulatory enforcement investigations involving companies, it is often clear from the commencement phase that this will be the most likely outcome, and dialogue throughout the investigation will have to be directed towards this outcome.

It should not be assumed that the process leading to a negotiated disposal is a smooth or simple one. Even in cases involving only one enforcement authority, the legislation and rules governing settlement and the calculation of penalties are complex. Although the discounts available for early settlement are potentially significant, the processes leading to them can involve successive rounds of proposals, counterproposals, representations and negotiations. In criminal investigations, in jurisdictions where it is possible to achieve negotiated outcomes as an alternative to prosecution, although the degree of scrutiny varies depending on which jurisdiction is concerned, such settlements will also be examined by a judge.

Complexity is multiplied where multiple authorities or jurisdictions are involved, or where it is possible that a finding, even if it does not involve any admission of liability, may fuel subsequent litigation from third parties such as erstwhile customers, employees or shareholders.

Although major investigations are unlikely to have progressed to the disposal stage without attracting at least some publicity, it is at this stage that press and political interest will peak. Enforcement authorities usually must make the outcomes of investigations public (and indeed corporate entities themselves may be obliged to do so if their securities are listed).

Other difficult questions arise with negotiated disposals. What will be the size of the fines, if any? For individuals, is there the prospect of imprisonment or other career-threatening penalties? Will it be possible to settle with all interested investigating authorities? For the corporate to bring matters to a close, will it be necessary to assist authorities in their pursuit of individuals? Will the disposal of the investigations mark the end of the matter, or simply the start of a new phase of litigation or the commencement of a long process of reporting to a monitor and heightened levels of regulatory scrutiny or supervision? What can be said publicly by the subjects of the investigations?

1.3.4 Compliance programmes

During the tenure of Lisa Osofsky as Director of the SFO, the effectiveness of a corporate organisation's compliance programme has assumed even greater

© Law Business Research 2021

importance in concluding an investigation through a DPA and its terms. In January 2020 (shortly before the largest settlement yet reached through a UK DPA, between the SFO and Airbus), the SFO published guidance[93] about how and when it will evaluate compliance programmes maintained by corporate organisations it is investigating. It is not prescriptive, must be read in conjunction with a raft of other guidance about whether immediate prosecution or a DPA will be the most appropriate option and leaves SFO prosecutors with significant latitude as to how much credit corporate organisations should receive for their compliance arrangements. However, it makes clear that the SFO will start assessing corporate organisations' compliance programmes at an early stage of investigations and that a DPA may still be possible even where deficiencies are identified.

The guidance states that the SFO is interested in seeing whether the corporate organisation concerned is taking a 'genuinely proactive' approach to compliance and in the past, present and proposed future state of compliance programmes and is more concerned with amelioration and demonstrable action than perfection. The guidance also reinforces that the SFO's assessment will be based on the principles set out in the guidance issued by the Ministry of Justice in relation to what will amount to 'adequate procedures' under section 7 of the Bribery Act 2010.[94] These indications are consistent with the settlements reached in DPAs concluded since 2014. The guidance also suggests a possible departure from previous practice in relation to the appointment of monitors, stating that where DPAs include provisions about compliance programmes, the SFO is likely to require the appointment of an external monitor (at the corporate organisation's expense) to verify that required improvements are made. There are signs in DPAs agreed so far and in pending cases that may lead to DPAs that the SFO is committed to imposing this requirement in practice.

July's *G4S Care & Justice Services* DPA was unusual in requiring an external 'reviewer' for three years, to review and report to the SFO on the quality and success of G4S's corporate renewal programme and the other associated compliance measures. This is arguably the closest the United Kingdom has come to imposing a monitor, a 'deferred prosecution agreement with real teeth',[95] which is an established feature of DPA settlements in the United States, when a company's remediation and compliance improvement efforts are considered inadequate or the misconduct was pervasive throughout the organisation.

In the guidance on 'Deferred Prosecution Agreements' published on 23 October 2020, there is a section on the relevance of a company's compliance

93 SFO Operational Handbook, Evaluating a Corporate Compliance Programme, January 2020.

94 Ministry of Justice, The Bribery Act – Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing, March 2011.

95 Lisa Osofsky, SFO Director, speech at the Royal United Services Institute, Future Challenges in Economic Crime: A View from the SFO, 8 October 2020, https://www.sfo.gov.uk/2020/10/09/future-challenges-in-economic-crime-a-view-from-the-sfo/.

© Law Business Research 2021

programme to the DPA process. In terms reminiscent of the DOJ's updated guidance,[96] it states: 'A compliance programme must be proportionate, risk-based and regularly reviewed and tested, and the Company should be able to evidence that its programme has these traits, is adopted at board level and is sufficiently well resourced.'[97] It concludes: 'Where appropriate, the SFO may bring in external resources to assist in the assessment of the Company's compliance programme.'[98]

With these themes in mind, we turn now to a detailed consideration of each stage in the chapters that follow.

96 DOJ, Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

97 SFO Operational Handbook, 'Deferred Prosecution Agreements', available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/.

98 Id.

© Law Business Research 2021

2

The Evolution of Risk Management in Global Investigations

William H Devaney, Joanna Ludlam, Mary Jordan and Aleesha Fowler[1]

Introduction 2.1

This chapter addresses the myriad potential avenues for a control environment to be compromised and for an area of risk or investigation to be identified, either proactively or reactively, by a corporate. It also highlights key developments and changes we have observed in the past year regarding risk management and global investigations. First, the chapter provides a close look at some of the primary triggers or sources of investigations for corporates from both an internal and external perspective. Second, it considers some of the challenges in conducting remote investigations in a work-from-home environment. Third, we discuss developing environmental, social and governance (ESG) issues – an increasing focus for law enforcement and regulatory authorities. The chapter concludes with a brief discussion on a question commonly asked by many corporations today: which corporate function (e.g., legal, compliance, or both) should be responsible for overseeing and conducting which types of investigations?

Sources and triggers of corporate investigations 2.2

Corporate investigations can be triggered by internal and external sources. Corporations often spearhead their own investigations in response to whistleblower reports concerning actual or suspected violations of law or company policy, or to assess the scope of potential problems and risks identified in routine due diligence, compliance reviews, and financial audits. However, corporations may also find themselves the targets of investigations commenced by law enforcement and regulatory authorities, such as the US Department of

1 William H Devaney and Joanna Ludlam are partners, and Mary Jordan and Aleesha Fowler are senior associates, at Baker McKenzie LLP.

© Law Business Research 2021

Justice (DOJ) and the UK Serious Fraud Office (SFO). External investigations can also arise from customer or competitor complaints, media reports or even changing political and policy agendas. We describe these and other common triggers or sources of investigations below.

2.2.1 Internal investigations

2.2.1.1 Internal whistleblowers

A substantial proportion of matters under investigation arise through a company's own policy and process for whistleblower complaints, such as through employee helplines, staff exit interviews and voluntary communications by current and former employees.

Most corporations today have a reporting mechanism through which employees, customers and members of the public can report (sometimes anonymously) actual or potential problems that pose risk to the company. The number of whistleblower complaints a company receives does not necessarily reflect the health of a company or its ability to detect risk. For example, a small number of complaints may reflect a company's strong compliance culture, or, conversely, a culture in which employees hesitate to make complaints out of fear of losing their jobs. On the other hand, a significant flow of concerns may reflect a more risk-aware body of employees who feel free to raise issues without jeopardy, or a body of employees who do not take compliance seriously and face no consequences for escalating frivolous complaints.

Reports suggest that an increasing number of employees in the United Kingdom have been blowing the whistle as a direct result of the covid-19 pandemic. The issues observed in this increase relate to such topics as abuse of the furlough and business support schemes; unsafe working environments; regulatory breaches caused by reduced supervision as more employees work remotely; and breaches emanating from economic and financial hardship brought on by the pandemic.[2] We are also seeing an increase in whistleblowing activity in the United States, Europe and the United Kingdom relating to social issues, including (but not limited to) diversity and inclusion, inequality, under-representation and discrimination.

Greater protection is being built in for whistleblowers by legislative changes, which may further increase the number of concerns we see raised.[3] For example, the Whistleblower Protection Directive is due to be implemented by EU Member States by 17 December 2021, and this will give protection to any person working in the private or public sector who makes a report regarding an alleged breach of EU law in a work-related context. The protection is wide and includes all current, former and prospective employees as well as contractors, unpaid trainees or volunteers. It applies to all businesses and government bodies

2 'Now is the Time to Embrace Whistleblowers', *Financial Times* (21 Sep. 2020).

3 This legislation applies to internal and external whistleblowers of a corporation.

© Law Business Research 2021

with 250 or more employees from 17 December 2021,[4] and UK and US companies with a footprint in the European Union will need to consider whether their whistleblower policies and procedures are sufficient to meet new standards.

See Chapters 19 to 21 on whistleblowing

Audits and reviews 2.2.1.2

Internal investigations may also be triggered by periodic audits and reviews. Many companies must by law conduct some form of internal audit or review concerning the truth and accuracy of their financial books and accounts. These audits are typically conducted annually by an independent audit firm, and the results are usually recorded in a written report. If any errors, gaps or other potential risks are identified, a company may decide to investigate and remediate any problems before the next report.

Corporations often conduct internal reviews to assess whether and to what extent their policies and procedures are adequately designed to detect and remediate risk. These reviews (risk assessments) can be performed by a law firm, or by a company's internal legal or compliance function (albeit with some privilege concerns for assessments conducted without counsel). Like financial audits, corporations may choose to investigate problems identified in these reviews, especially those that pose the greatest legal, financial or reputational risk to corporations and their business.

Transactional due diligence 2.2.1.3

Corporate transactions, such as mergers, acquisitions and joint ventures, are another common trigger for internal investigations. Corporations customarily conduct due diligence to identify any hidden risks presented by a target or counterparty. Particular attention should be given to areas that can give rise to successor liability.

While a corporation should consider various factors before entering into a transaction, some of the common due diligence considerations include whether the other entity:

- is sanctioned or has been subject to economic sanctions within the past five years;
- has a robust compliance programme that adequately accounts for relevant risks;
- is owned or controlled by a government official or a government body;
- has significant financial debts or liabilities;
- has been the subject of an external investigation brought by a regulator or law enforcement authority; and
- has been the subject of any litigation involving fraud or other allegations of illegality within the past five years.

4 It will further extend to businesses and government bodies with 50 or more employees by 17 December 2023.

© Law Business Research 2021

Pre-transaction due diligence in the above-listed areas (and others) is crucial. This is especially so due to the disruption and rapid change impacting businesses and corporate supply chains due to the covid-19 pandemic. Many industries face new inherent risks in their business (for instance, due to factors such as increased digitisation, reduced time spent vetting new business partners and ventures, or higher costs paired with reduced supply forcing businesses to make fast decisions on key issues). Conducting thorough and well-timed due diligence has never been more important to reduce the risk of entering into a transaction that could be financially and reputationally damaging, and to provide leverage to companies that later find themselves in the crosshairs of a government investigation. For example, in its FCPA Corporate Enforcement Policy, the DOJ has stated that there is a presumption of declination for an acquirer that conducts effective pre-transactional due diligence, remediates, folds the acquired entity into its compliance programme and voluntarily discloses the conduct.[5]

Whatever risk factor is being investigated, not only the primary due diligence activities t, but also the response to the information delivered by standard or enhanced due diligence, may stimulate wider investigation. The initial response separates the strong organisation from the weak and moves compliance culture from a tick-box habit to best-in-class governance and control.[6]

2.2.2 External investigations

2.2.2.1 Contact by regulatory and law enforcement authorities

In the UK regulated sector, where ongoing open and transparent dialogue is expected between corporations and their regulators, it is comparatively rare for a business to find out about issues for the first time as a result of unilateral contact from a regulator. Ordinarily, the regulated entity's report to the regulator leads to further investigation. By contrast, however, contact from prosecutors, competition authorities and, in certain circumstances, civil litigants, may occur without prior warning. In the United States, corporations frequently learn about an investigation for the first time from prosecutors, and criminal referrals from regulatory agencies to the DOJ are common.

But all companies, regardless of where they are located, should ask the following initial questions when approached by an authority:

- Is the company a target or subject of the inquiry, or is the authority simply looking for information from the company related to another's conduct?
- What information is the authority looking for?

5 Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, US Department of Justice (DOJ), Justice Manual (JM) § 9-47.120; A Resource Guide to the US Foreign Corrupt Practices Act, Second Edition (2020), 29 (discussing pre-transactional due diligence in context of successor liability). See also DOJ, Opinion Release 14-02 and Opinion Release 08-02.

6 For further information on tools and resources available to firms to assess and manage risk during a transaction, see the fifth edition of *The Practitioner's Guide to Global Investigations*, p. 31 et seq.

© Law Business Research 2021

- In what formats is the authority seeking information (e.g., emails, text messages, interviews)?
- How much information is the authority seeking (e.g., from the past 10 years)?
- Is the authority interested in a specific business line or area of the company?

Another initial question companies should ask is whether the investigation is being carried out by a regulator or prosecutor. A company may be inclined to treat these two types of organisations synonymously, but they discharge different duties, possess different (although sometimes overlapping) powers, and have different expectations regarding cooperation. Accordingly, a company's approach to dealing with a regulator may need to differ from its response to dealing with a criminal prosecutor's office.

A prosecutor investigating a matter is normally seeking evidence to decide whether a crime has occurred and whether individuals or the company should be criminally charged. If it proceeds with a prosecution, it carries the burden of proof (with certain limited jurisdictional and subject-matter exceptions). Apart from specific mandatory reporting regimes,[7] there is no obligation to volunteer information about misconduct to a prosecutor in the absence of a subpoena, warrant or other court order. It is an offence to obstruct an investigation, but obstruction does not extend to failure to volunteer evidence in the absence of compulsion; however, the provision of false, misleading or incomplete information to a prosecutor could amount to an offence of obstruction of justice in the United States or perverting the course of public justice in the United Kingdom. In the United States, it is a crime to destroy evidence, even in the absence of compulsion or the initiation of a proceeding, when the purpose is to avoid its disclosure in an anticipated criminal or regulatory investigation or proceeding.[8] Further, the Fifth Amendment right against self-incrimination extends only to individuals, not corporations. Therefore, ancillary Fifth Amendment protections, such as the act of production doctrine, which permits an individual to hold back documents if the mere act of producing them, as opposed to their content, will be incriminating, does not apply to corporates.[9, 10]

See Chapters 5 and 6 on beginning an internal investigation

7 e.g., the obligation in the United Kingdom to submit suspicious activity reports under s.330, Proceeds of Crime Act 2002.

8 See 18 U.S.C. § 1519.

9 See *United States v. Hubbell*, 530 U.S. 27 (2000).

10 For the UK financial services industry, this is to be contrasted with the duty of open and co-operative dealings with the FCA, whereby evidence of a control breach would be reported without delay and significant regulatory implications could arise from a failure to do so. A US corporate's duty to disclose is limited. See Chapters 9 and 10 on co-operating with authorities.

© Law Business Research 2021

In dealings with UK prosecutors, while opportunities for mitigation and leniency exist through demonstrable co-operation[11] (and a company may regret not being able to obtain co-operation credit later on), co-operation is a matter of pragmatic choice rather than legal obligation. The starting point remains unchanged: under what valid power does the prosecutor seek the evidence, what are the company's reasonable defences and how tactically does the company respond? While principles of co-operation with government agencies in the hope of gaining leniency or mitigation are more clearly defined and have a longer tradition in the United States, the general rule of law remains intact and questions of powers, defences and tactics are no less germane.[12]

Where a prosecutor, police or investigative agency, competition authority or other public body serves a subpoena, order or warrant entitling it to documents and electronic information, or to enter, search and seize, monitor or restrain, the challenge for the affected organisation is twofold: (1) to provide information or permit access and activity within the confines of the power granted; and (2) to ensure the company is not left behind (and preferably remains in front) in its own understanding of the relevant facts.

See Chapter 11 on production of information to authorities

In the United States, grand jury subpoenas are the most common tool prosecutors use to gather information against a corporation in a criminal investigation. Various civil and regulatory enforcement agencies, such as the US Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission, may also issue subpoenas. General principles to follow when responding to a subpoena include issuing hold notices to the relevant employees and, if appropriate, third parties, to ensure that all information requested or potentially relevant to the enquiry (emails, other electronically stored information, hard-copy documents, etc.) is retained; controlling insider lists to identify those now aware of facts that may constitute inside information; preparing witness lists (to ensure they do not receive updates or advice on the matter, which may contaminate their evidence); and giving consideration to the treatment of witnesses (whether they require independent legal advice, or should be removed from the office environment through suspension

11 In the United Kingdom, with the introduction of the Serious Fraud Office's deferred prosecution agreement power in 2014.

12 There is no legal obligation to co-operate in an investigation in the United States. Under the Principles of Federal Prosecution of Business Organizations, however, a corporation's willingness to co-operate is a factor in determining whether to charge the corporation. But, a corporation's refusal to co-operate alone is not justification for prosecution. See JM § 9-28.700. Formal obligation aside, from a more pragmatic perspective, US and UK entities under a deferred prosecution agreement or non-prosecution agreement, or parties subject to monitorships, may find they have little choice but to disclose, as might a member of the heavily regulated financial services sector, which could face adverse findings in relation to the duty to deal openly and transparently with its regulator. Further, the FCPA Corporate Enforcement Policy, which informally applies to offences outside the FCPA, requires voluntary disclosure for a corporation to receive its full benefit. See JM § 9-47.120.

© Law Business Research 2021

or relocation so as not to risk evidence tampering, collusion or undue influence over other witnesses). In a criminal matter, defence counsel will almost always engage with the prosecutor to determine the company's status as a witness (potentially having relevant information, but no criminal liability), subject (the largest category, in which the government does not yet have sufficient information to determine criminal liability) or target (the government is gathering evidence to bring criminal charges against the company).[13] Counsel will also almost certainly work to narrow the scope of the information requested.

A number of important general principles apply also to the execution of search warrants and the conduct of dawn raids:

- The order or warrant must be reviewed to ensure that the party serving or executing it has the requisite power. (Does it catch the correct entity? Is it the correct site or office? Are the search area and the items the authorities are searching for described with the requisite particularity? Are there date or time discrepancies? Is it signed or executed? In the United Kingdom, does it bear the correct court seal? Does the person conducting the inspection have the requisite authority in that jurisdiction?)
- All relevant parties need to ensure the full scope and context of the search is understood (and where electronic searches are undertaken, endeavour to agree on relevant keyword searches and the exclusion of out-of-scope material, such as privileged documents or personal data).
- As with a subpoena, it will generally be necessary to issue hold notices immediately after receipt of the order or warrant with instructions not to destroy or spoil evidence or to give false or misleading information. As well as the obvious practical importance of preserving relevant evidence, there is also significant value in being seen to co-operate as an initial response.
- Individuals executing the order should be subject to identity verification to ensure that execution is in accordance with the terms of the order and that their identification is recorded (in the event that the order is breached and an individual's identity becomes relevant to any proceedings arising as a consequence).
- Staff, including reception and a designated dawn raid team, should be trained in advance as to how to conduct any interaction with investigators from the moment of first access to the premises. This includes training and instruction on not answering apparently casual questions on the subject of the search. The informal question to the unready on the walk along the corridor is a well-established source of information for experienced investigators. Any questions asked of staff and their responses should be noted. Employees may be informed of their legal rights not to speak to investigators and their right to counsel. Additionally, if the company is willing, the employees may be told that the company will provide legal counsel to them at no cost if investigators wish to speak to them or if they are later contacted. The company

13 See also JM § 9-11.151, defining 'target' and 'subject'.

© Law Business Research 2021

may not, however, instruct employees not to speak to investigators. That is the employee's choice.

- A separate room should be set aside as a base for investigators and discussions between legal function representatives and the visitors so that debate and investigative activity does not take place within earshot of those under investigation.
- Local IT support (technology, plus a nominated IT representative) should be made available in the same room to ensure the IT environment can be explained to investigators and accessed. A log of access and copies of materials reviewed or seized should be made as the matter progresses so that a company's own investigators and lawyers can subsequently review the same material and evaluate compliance with the order or warrant.
- A written log should be kept of all places searched, items seized and staff interviewed. Legal counsel should be present, if possible, to assert objections based on the attorney–client privilege, to identify commercially sensitive information or the sensitive personal information of customers or employees and to object if the search exceeds its authorisation. None of this, however, can be obstructive. The remedy for an improper search or seizure is to be had in court, not while the search is being conducted.
- Seek to agree with the investigators in advance on the definition and scope of principles such as legal privilege, commercial confidentiality, relevance, personal data and other material the company would contend falls outside the terms of the order, and to a protocol for handling these materials during and after the search.
- Consider whether it is necessary and appropriate to prepare a press release or public disclosure (e.g., stock exchange announcement) confirming the on-site inspection and its scope or purpose. In the United States, it may be advisable to convene a 'town hall' meeting with employees to discuss the search and the looming investigation, but in the United Kingdom, this practice is not favoured as it could tip off individuals who do not intend to comply, triggering evidence tampering or impacting the integrity of witness testimony.

See Chapters 38 and 39 on publicity

2.2.2.2 Media coverage

Unexpected media reports or more aggressive or intrusive media behaviour (such as undercover investigative journalism) can trigger an investigation in extremely pressurised circumstances. The media outlet running the story will often have completed its investigation before the company is aware of the matter. In the worst cases, the first a company learns of the facts is in the publication or broadcast, although various broadcasting codes and voluntary editorial principles encourage the opportunity for a right of reply, so most coverage will follow a short period of discussion of content between the media and the subject of the story, yet not enough to accommodate an investigation and fully informed response.

© Law Business Research 2021

Even if a company is already aware of an issue and has undertaken some investigation before the issue becomes public, sudden and intense media scrutiny may require a company to adjust its response to protect its legal position and reputation, and to be seen to understand the public demand for resolution. For example, companies that were initially intending to adopt a passive approach to an issue or undertake a low-key investigation may change this response once the media takes up the issue.

In 2020, a UK-based fashion retailer, Boohoo, was the subject of various newspaper articles that alleged the company's clothes were made in factories that employed workers at below minimum wage. According to these news sources, workers at the Boohoo factories worked under squalid conditions, and those in Pakistan were paid as little as 29 pence per hour. These allegations contradicted both Boohoo's modern slavery statement (proclaiming the company took a 'zero-tolerance' approach), and the company's expectations that its suppliers adhere to a code of conduct that included a living wage requirement for all workers. Just a few days after the articles were published, it was reported that Boohoo's shares lost more than a fifth of their value.[14] In addition to this financial hit, the National Crime Agency, HM Revenue and Customs, the Home Office and Health and Safety Executive (all UK public authorities) worked together to investigate the UK factories at issue. Boohoo rapidly appointed experts to consider the allegations against the company and oversee improvements to its supply chain and business practices.

As this case highlights, adverse media reports about a corporation's business operations can result in reputational damage, financial harm and increased scrutiny from regulatory and law enforcement authorities. Companies do not always have time to adequately respond to these reports, especially in an environment where news travels at a fast pace. From a practical point of view, there is an immediate balance that companies must strike between taking the time to conduct a thorough investigation, and responding to urgent media and public enquiries.

Companies can minimise the negative consequences that accompany adverse media reports by proactively implementing a crisis management plan. This should not only account for how the company will respond to the media and its customers, but also how the company investigate the allegations, in both the short and long term. Setting up an investigations steering group and having effective policies and processes in place that are observed by senior management will ensure emergency investigations are not obstructed by administrative chaos.

See Chapters 38 and 39 on publicity

Politics and political agendas 2.2.2.3

The regulatory agenda is often set, adjusted or inflamed by the political climate, such that external regulatory or criminal investigations would not commence but for political pressure or the sudden availability of funding. The political

14 'Boohoo shares tumble on concerns over factory conditions', *Financial Times* (6 Jul. 2020).

© Law Business Research 2021

agenda itself may change overnight in the face of public or media pressure. Two relevant examples of this are Brexit and the election of President Biden.

It remains to be seen how the politics surrounding Brexit will impact the authorities' investigation activity. Following the end of the transition period,[15] many of the mechanisms needed for close co-operation between UK and EU law enforcement agencies remain in place. At a policy and strategy level, the United Kingdom's role in EU criminal justice arrangements is much diminished (to the same level of other non-member states, such as Norway), but the United Kingdom still has access to key investigative tools that were available before Brexit, such as the ability to obtain evidence and to secure the surrender of suspects from EU member states, and to access intelligence and information such as criminal records. Turnaround times may become slightly longer, but the impact overall is much reduced compared with what may have been the case in the event of a no-deal Brexit, and are in some respects difficult to separate from the impact of the covid-19 pandemic, which has posed issues for investigation timing and accessibility to data.

The FCA and the SFO are UK-focused agencies and their mandates are broadly unchanged by Brexit, so in that sense we do not expect it to have a direct, immediate impact on UK regulation and enforcement, although the transition out of the European Union and the change in financial services regulation that comes as a result of the United Kingdom's independence will be a key area to watch. The Financial Services Act of 2021 (FSA) was the first major piece of UK primary legislation addressing the issues relating to financial services and financial regulation arising from Brexit. It makes amendments to rules regarding access to financial services markets for overseas funds and third country investment firms, it amends the EU Benchmark Regulation, and it amends the Market Abuse Regulation to increase the maximum sentence for criminal market abuse. In July 2021, the UK government released 'The New Chapter for Financial Services', a paper setting out the United Kingdom's vision for its financial services sector, with further updates expected in 2022. The paper targets sustainability, green credentials and technology, and the United Kingdom's post-Brexit planning to date is very much focused on ESG.

In the United States, the Biden administration has made clear its intention to address vulnerabilities in, and strengthen the resistance of, critical US supply chains. In February 2021, President Biden signed Executive Order 14017 (America's Supply Chains), marking the first comprehensive, government-wide policy specifically focused on supply chains. Pursuant to that order, a series of reviews were conducted to assess risks and vulnerabilities in four sectors: semiconductor manufacturing and advanced packaging; large capacity batteries (e.g., electrical vehicle batteries); critical minerals; and pharmaceutical ingredients.

15 The transition period (sometimes called the implementation period) expired on 31 December 2020.

© Law Business Research 2021

In June 2021, a set of reports was released that summarised the key findings from these reviews and made policy recommendations to address identified supply chain risks.[16] The reports included various recommendations related to human rights, such as a recommendation for new legislation aimed at reducing the impact of forced labour and other human rights abuses in supply chains that manufacture critical minerals and materials. The reports also make recommendations related to environmental sustainability, specifically noting that the United States 'must work with allies and partners to diversify supply chains away from adversarial nations and sources with unacceptable environmental and labor standards', and that US investments abroad 'must incentivize environmentally and socially responsible production'.[17] These recommendations align with recent global developments in ESG issues.

Corporations with US supply chains should closely monitor the developments of the recommendations made in the reports. Should these become law, companies must develop a process for identifying, evaluating and remediating supply chain risk – which will require a review or investigation by corporate legal and compliance functions.

Additionally, on 3 June 2021, President Biden issued a memorandum stating that the fight against corruption was a 'core' United States national security interest and directing an inter-agency review process aimed at increasing the ability to fight corruption within the United States and abroad. It is likely that this review will result in increased resources to fight corruption, greater inter-agency co-operation in the United States (including among intelligence and law enforcement agencies), greater international co-operation, and a heightened emphasis on increased transparency in financial transactions. This memorandum follows the implementation of other recent measures such as the Anti-Money Laundering Act of 2020 (AMLA), enhancing US prosecutors' ability to seek financial information from non-US banks, the DOJ's Kleptocracy Asset Recovery Initiative and its China Initiative. Taken together, these would also portend an increase in corporate investigations.

Investor complaints and shareholder derivative lawsuits 2.2.2.4

Complaints raised by shareholders can trigger twin legal activities: a defence strategy in cases where issues of liability are plainly articulated and facts are

16 See The White House, 'Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017' (8 Jun. 2021).

17 White House Briefing Room, Fact Sheet, 'Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities' (8 Jun. 2021). Baker McKenzie has been closely following the governance recommendations made in these reports on its Global Supply Chain Compliance Blog, which can be found online at https://supplychaincompliance.bakermckenzie.com/2021/06/16/biden-administration-supply-chain-reports-deeper-dive-1-the-expansion-of-regulatio-over-responsible-sourcing-of-minerals-and-corruption-in-supply-chains-on-the-horizon/.

© Law Business Research 2021

either already established or may be simply assessed; and separate investigations into wider concerns raised by the complaint, or where the facts are far from clear and the allegations cannot be adequately responded to without an investigation.[18]

A major sensitivity in matters of this nature, which can be overlooked in pursuit of the defence of the civil action, relates to the ongoing disclosure and transparency obligations arising from stock exchange listing rules. It is one thing to investigate sufficiently to position a company to defend litigation on the balance of probabilities, or to be able to respond to a letter of concern or questions from the floor in an annual general meeting, but another to investigate to a point where a public statement can be made with sufficient accuracy to satisfy the reasonable investor test.[19]

While a company may wish to respond speedily to concerns raised by an investor, dealing with investor complaints carries a further layer of complexity and a balance needs to be struck between the urgency to make a statement to the market and the time needed to investigate facts sufficiently to make an adequately precise and informative one. The publication of false or misleading statements through inadequate or incomplete investigation simply increases the range of potential legal liabilities and further delays resolution.

2.2.2.5 Customer and competitor complaints

Complaints made by customers and competitors constitute another category of triggers of external investigations. Customers and competitors may refer complaints to law enforcement, regulators, consumer bodies and ombudsmen. Individual incidents may be sufficiently problematic to merit investigation in their own right. However, even with low-value customer complaints, there comes a point where a volume of similar-fact criticisms raise concerns as to the fairness of underlying sales processes and adequacy of complaints handling systems, or perhaps even broader questions of breaches of systems or controls, that may combine to catch a regulator's attention and create reputational risk.

While it might be hoped that a company's own monitoring of complaints levels and sources should trigger deeper investigation into the underlying issues, it will sometimes take unilateral regulatory enquiry and enforcement processes to bring about a non-voluntary, full evaluation, including thematic reviews, 'skilled persons appointments',[20] market studies and industry sweeps. Significantly, the

18 In the United States, shareholders can generally bring a derivative lawsuit on behalf of a corporation if they have provided notice to the board of directors and the board has determined that the lawsuit is in the best interest of the company.

19 In the United Kingdom, information a reasonable investor would be likely to use as a basis for his or her investment decisions. See Financial Services and Markets Act 2000 (FSMA) and Market Abuse Regulation, Article 7 relating to inside information. These provisions require a high degree of precision in the accuracy of factual statements.

20 Under FSMA, s.166, the FCA has the power to commission a report from a third party (skilled person) about aspects of a regulated firm, usually focusing on specific issues about which the

© Law Business Research 2021

company's in-house investigators will not set the parameters of the investigation (though they can add significant value in debates with regulators over scope and process and may be heavily involved in the activities that follow, by partnering with the external firm in a skilled person's review, for example). The in-house function will remain critical in the parallel process of evaluation of evidence so that advice may be taken to respond to regulatory or legal liability.

A complaint or concern raised by a participant in the same market raises a number of wider risks colouring the subsequent investigation. In certain ways, a competitor complaint has more in common with whistleblowing (and may even be regarded as such by authorities) in that it may create forms of protected disclosure, confidentiality obligations and behavioural expectations from particular authorities. This is certainly the case in competition matters where leniency or immunity is sought following a self-report to an authority following a tip-off or complaint by a competitor. This immediately limits the scope for communication of issues (including even the existence and subject matter of the investigation) among staff and will have a particular bearing on the management of evidence, including witness handling and interviews. It will also affect the extent to which there may be ongoing communication outside the organisation where, for example, witnesses may exist within the competitor organisation but further dialogue is not possible without the consent of, and careful choreography by, the relevant authority.

The challenges of conducting remote investigations 2.3

The covid-19 pandemic has led to a shift towards remote investigations. While they offer certain advantages (e.g., a cost-effectiveness), they pose several challenges and risks for companies. For example, remote investigations create fertile ground for hackers looking to steal company information or disrupt a company's information systems. Working from unsecured Wi-Fi networks creates the risk of confidential and privileged information being intercepted. Also a witness can surreptitiously record an interview or have others in the room out of sight, jeopardising confidentiality and even the attorney-client privilege. At the same time, company lawyers need to ensure that unauthorised people are not in their rooms during remote interviews. Additionally, the sharing of sensitive documents presents risks and challenges in a remote environment. And witnesses who need to be deposed or interviewed in connection with investigations might not feel comfortable being transparent and sharing necessary information via third-party teleconferencing software services. Conversely, interviewers lose a level of human connection helpful for gaining witnesses' trust, effectively confronting a witness – particularly a recalcitrant one – and

FCA has concerns or wishes to analyse in greater detail. The skilled person may be appointed by the FCA, or the FCA may ask the regulated firm in question to put forward their preferred choice of candidate for approval by the FCA.

© Law Business Research 2021

judging credibility. Finally, remote interviews, particularly government interviews, are much more difficult for defence counsel who are not in the same room as their clients.

Corporations will need to account for these and other similar challenges and the risks they pose as remote work becomes the norm. Companies may consider the following:

- offering legal and compliance employees training on how to conduct investigations remotely;
- procuring and investing in secure information software to prevent, minimise and monitor hacking and data leaks;
- establishing a policy and procedure for protecting and transmitting company information both internally and externally; and
- implementing a disciplinary process for employees that violate company policy and procedure related to the handling and transmittal of company information.

2.4 ESG issues

See Chapter 47 on ESG

Corporate investigations (whether triggered internally or externally) have traditionally focused on compliance. The investigations that tend to make headlines and soak up corporate resources are those concerning an entity's alleged violation of laws related to bribery, corruption, securities fraud, money laundering and similar misconduct that pose significant legal risk. These investigations are often global, involve some of the most active law enforcement and regulatory authorities, and can result in large monetary settlements and criminal penalties. But the nature and scope of corporate investigations is slowly evolving as companies face increasing pressure to adopt and report on standards related to ESG issues, such as those concerning human rights, corporate citizenship, diversity and environmental sustainability.

Corporations have historically viewed ESG issues as a set of loose, voluntary standards that pose little to no legal risk. While this might have been true 10 years ago, it is certainly not the case today, with shareholders, employees, consumers and other stakeholders demanding that corporate boards make ESG a priority in corporate operations, and regulatory authorities around the world increasingly requiring corporations to report on their ESG activity. For example, the SEC announced that a key priority is implementing new ESG and climate disclosure requirements for registered companies. In discussing their importance, Allison Herren Lee, then acting SEC Chair, stated that it is 'time for the SEC to lead a discussion – to bring all interested parties to the table and begin to work through how to get investors the standardized,

© Law Business Research 2021

consistent, reliable and comparable ESG disclosures they need to protect their investments and allocate capital towards a sustainable economy'.[21]

In the United Kingdom, the Bank of England and the FCA are similarly leading the way in making ESG a central regulatory and supervisory consideration.[22] The United Kingdom is currently expected to be one of the first countries in the world to make disclosures that are aligned with the Taskforce on Climate-related Financial Disclosures, intending to make it fully mandatory by 2025. Already, the EU's Regulation on sustainability-related disclosures in the financial services sector (SFDR) came into force in March 2021, imposing ESG transparency and disclosure requirements on financial institutions. The SFDR applies to all businesses offering financial products on the European market so it is a good example of the general direction of international financial standards. Its overarching aim is threefold: (1) to prompt financial services providers that manage client assets or advise clients on investments to integrate ESG into their processes and to inform their clients on ESG matters; (2) to create a harmonised regulatory framework to ensure a level playing field across the financial services sector to enable investors to compare ESG factors; and (3) to require transparency from firms regarding their ESG policies through precontractual disclosure requirements, disclosures on their website and periodic reporting.

These developments have had (and will continue to have) an impact on what companies investigate and how they approach investigations. For example, corporate counsel of companies subject to existing and contemplated ESG disclosure requirements will need to investigate (1) the actions the company has taken in the area of ESG, (2) the ESG-related statements and commitments the company has made to the investing public on its website or in other publicly available materials and (3) whether and to what extent the company's actions in the area of ESG align with its published statements and commitments. Some investigations will not be driven by fear of regulatory action at all, but by corporations trying to demonstrate to consumers, employees and other stakeholders that they are living-up to their ESG claims or stakeholder expectations. Whatever the driver for the investigation, to be effective, ESG investigations will require corporate counsel to remain up to date on growing and fast-changing standards and requirements.

21 See Securities and Exchange Commission Public Statement, Regulation S-K and ESG Disclosures: An Unsustainable Silence, available at https://www.sec.gov/news/public-statement/lee-regulation-s-k-2020-08-26.

22 The Bank of England's Prudential Regulatory Authority Supervisory Statement (SS3/2019) set expectations for financial institutions regarding climate risk across governance arrangements, risk management, stress testing and scenario analysis and disclosure. The FCA's business plan for 2021–2022 states the FCA's commitment to assisting the government to find a market-based transition to a low carbon, sustainable future, with a particular focus on the marketing and disclosure around ESG-related products and risks.

© Law Business Research 2021

2.5 Corporate legal and compliance functions: who should investigate?

Corporate investigations often fall within the remit of legal and compliance departments. Some companies keep the functions separate, others assign similar and overlapping responsibilities to them, making them difficult to distinguish. A common question we receive from companies that have both functions is which department should be responsible for conducting investigations?

There is no single, straightforward answer, which will depend on the type of investigation, a corporation's resources (including staffing and technology), and the nature and scope of the problem. Generally speaking, the legal department plays a reactive role, spearheading investigations after a potential problem has been identified to mitigate a company's overall liability. For example, legal departments often lead investigations concerning actual or suspected violations of anti-bribery and corruptions laws, which can lead to significant criminal and civil penalties, and often require coordination and co-operation with the authorities. In addition to their skill set, legal departments will also often lead in these types of investigations, and similar matters, where it is important to protect the investigation under the attorney client privilege.

The compliance department often plays a more proactive role, overseeing and managing corporate behaviour to prevent wrongdoing. Compliance departments tend to lead investigations focused on detecting risk and ensuring the company's current compliance framework (e.g., its company's policies and procedures) is adequately designed to prevent and respond to risk. For example, compliance departments are often asked to conduct periodic reviews and risk assessments, and to recommend general compliance improvements. Even with investigations or compliance efforts of this type, it is prudent for corporations to consider the nature, background and potential implications of the enquiry and whether it is better that they be led by lawyers to be covered by the attorney–client privilege.

Investigations are never straightforward, however, and in practice companies leverage the knowledge and resources of both the compliance and legal functions when conducting investigations. We see this play out in a number of areas, and most recently regarding ESG. Companies are being called on by stakeholders and government bodies to assess and report on their compliance with applicable ESG standards – for example whether and to what extent a company sources responsible goods and products, abides by human rights laws, and takes steps to reduce carbon emissions from its business operations. Ensuring a company's compliance with these standards is not a purely legal or compliance function: legal should be involved in ESG-related investigations because as we have highlighted, there are budding laws and regulations in various jurisdictions that allow for the enforcement of these standards; and compliance should be involved to identify and assess ESG risk and to track carefully these ever-evolving risks and to assess how the company's current compliance structure addresses them.

© Law Business Research 2021

3

Self-Reporting to the Authorities and Other Disclosure Obligations: The UK Perspective

Judith Seddon, Amanda Raad, Sarah Lambert-Porter and Matthew Burn[1]

Introduction 3.1

Whether, when and how a company should report potential misconduct requires an increasingly 'global' (in all senses of that word) view of the risks and benefits involved. Around the world, levels of enforcement action in relation to bribery and money laundering are increasing and remain high. International co-operation between authorities is being expanded and enhanced, and a growing number of jurisdictions are moving towards deferred prosecution agreements (DPAs) and formalised or protected whistleblowing regimes, as part of a general and growing trend towards incentivising corporate self-reporting.[2]

1 Judith Seddon and Amanda Raad are partners, Sarah Lambert-Porter and Matthew Burn are senior associates, at Ropes & Gray LLP in London.

2 In Lisa Osofsky's first speech as Director of the Serious Fraud Office (SFO), she referred to how the 'increasingly multi-jurisdictional and complex' nature of SFO cases makes co-operation to achieve global settlements all the more important. She said that '[s]trengthening and deepening the relationships that make this happen is going to be a major focus for me' and listed the newcomer countries to DPAs as part of that focus. Lisa Osofsky, SFO Director, speech at the Cambridge International Symposium on Economic Crime 2018, Jesus College, Cambridge (3 Sep. 2018), available at www.sfo.gov.uk/2018/09/03/lisa-osofsky-making-the-uk-a-high-risk-country-for-fraud-bribery-and-corruption/. Three years on, co-operation continues to be central to the SFO's strategy, and Lisa Osofsky regularly notes it as a priority. In 2019, she pointed out that '[p]rosecutors all around the world are realising how much we need each other if we are truly to do justice. So we are increasingly linking arms in the march against transnational fraud and corruption.' (Lisa Osofsky, 2 Sep. 2019, available at https://www.sfo.gov. uk/2019/09/02/cambridge-symposium-2019/), and in 2020 she noted: 'Our priority is to strengthen our international security relationships. It's a job we relish and for which we are well suited

© Law Business Research 2021

A firm's voluntary decision to self-report requires directors to evaluate the potential benefits and risks involved in doing so, while complying with their duties under the Companies Act 2006 to consider and act in the best interests of the company as a whole (and to comply with any other mandatory reporting obligations that may apply).[3] Key benefits of self-reporting include the ability to manage the timing and content of the information being provided to the authorities, the potential for securing a DPA (or other negotiated settlement), reducing any financial penalties, minimising or managing reputational fallout, and achieving an earlier and more predictable resolution than may otherwise be possible. Particular risks include potential disruptive and damaging action by investigating authorities, damage to share prices, the removal or suspension of senior management, costly internal investigations (including potential regulator involvement and the potential loss or waiver of privilege over key material) and potential civil litigation. The still relatively small body of decided cases in relation to DPAs in the United Kingdom, together with guidance setting out the circumstances in which they will be contemplated and entered into, provide some direction as to whether self-reporting may produce a negotiated outcome.

The stakes for individuals (usually directors) are also higher than ever in the United Kingdom – those working in firms regulated by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA) will need to consider how the United Kingdom's Senior Managers and Certification Regimes (SMCR) (introduced in respect of banks and insurers in 2016 and extended to all financial services firms in 2019) may provide those regulators with an easier route to regulatory enforcement action against them, in addition to any criminal and civil liability.

Frequently, questions as to how to deal with internal disclosures made by whistleblowers and, in those circumstances, whether, when and how to self-report matters to authorities, go hand in hand. Similarly, where a firm operates in multiple jurisdictions, any trigger of mandatory reporting obligations in one jurisdiction warrants careful consideration regarding corresponding mandatory or voluntary reporting in others – particularly in light of authorities' increasingly collaborative approach to (formal and informal) sharing of information.[4]

---

as we have, for many years, built up close partnerships around the world.' (Lisa Osofsky, 8 Oct. 2020, available at https://www.sfo.gov.uk/2020/10/09/future-challenges-in-economic-crime-a-view-from-the-sfo/).

3 Companies Act 2006, s.172.

4 For example, in the Corporate Co-operation Guidance, the SFO has set out certain indicators of good practice that they would expect to see in a co-operating corporate, including that an organisation should '[n]otify the SFO of any other government agencies, domestic or foreign, law enforcement or regulatory) by whom the organisation has been contacted or to whom it has reported', SFO Operational Handbook, Corporate Co-operation Guidance, p. 4, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

© Law Business Research 2021

Self-reporting is therefore a critical decision and can help to conclude regulatory intervention swiftly or even pre-empt it. The decision to self-report is seldom simple and typically involves balancing not only complex questions of fact and (criminal, regulatory and employment) law but also the risks and benefits of doing so. All these considerations also play out against the backdrop of an obvious tension between self-reporting with sufficient speed to obtain or maximise co-operation credit and the chance of a DPA on the one hand, and taking the time to investigate an allegation sufficiently to understand whether, when and what to report on the other. The Court of Appeal's 2018 decision in the *ENRC* case[5] emphasises the importance (for the purposes of asserting legal privilege) of recording clearly and in good time the points at which a firm considers that it is involved in the self-reporting process and that litigation or criminal prosecution is reasonably in contemplation.

This chapter examines how authorities are using and interpreting self-reporting and whistleblowing frameworks in the United Kingdom, and identifies key considerations for firms and their advisers. The extraterritorial reach of several pieces of key legislation (most notably the Bribery Act 2010 (UKBA)) and the comparatively aggressive stance of UK investigating and prosecuting authorities (principally the Serious Fraud Office (SFO)) mean that developments in the country are of interest to firms operating around the world, even if they are based, or undertake most of their activities, outside the United Kingdom.

Culture and whistleblowing 3.2

Self-reporting and whistleblowing are increasingly considered to be fundamental to and indicative of the culture of an organisation. In the wake of the financial crisis and more recent well-publicised instances of corporate misconduct, UK regulators and enforcement authorities have focused on culture as a strategic and supervisory priority.

The first DPA of 2021, agreed by the SFO and Amec Foster Wheeler Energy Limited (AFWEL) in June 2021,[6] elucidates the connection between culture and self-reporting, and the implications for companies that fail to self-report evidence of actual or potential misconduct. The DPA concerned bribery and

5 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp. Ltd* (*ENRC*) [2018] EWCA Civ 2006.

6 *Serious Fraud Office v. Amec Foster Wheeler Energy Limited*, unreported (25 Jun. 2021). The DPA was approved in principle by Lord Justice Edis at a private hearing at the Royal Courts of Justice on 25 June 2021. At the time of writing, the statement of facts underpinning the DPA remained subject to a reporting restriction order in light of the SFO's ongoing investigation into individuals. Edis LJ's judgment was published on the SFO website on 1 July 2021 and is available at https://www.sfo.gov.uk/download/amec-foster-wheeler-energy-limited-deferred-prosecution-agreement-judgment/. For the first time, the DPA and judgment bear a heading making it clear that each document relates solely to the culpability of AFWEL and not to that of any individual in respect of whom the court did not make any findings of fact.

© Law Business Research 2021

corruption that occurred in several countries between 1996 and 2014, when AFWEL was known as Foster Wheeler Energy Limited (FWEL). As part of the DPA, John Wood Group PLC, which acquired AFWEL after the SFO's investigation began, has undertaken to meet its liabilities. The evidence was that FWEL and its then parent company, Foster Wheeler Limited (FWL) knew about the potential internal corrupt conduct in Saudi Arabia at least as early as October 2007 when its lawyers, Baker Botts, submitted a report that was discussed (and minuted) at a FWL board meeting in November 2007. At that meeting, Baker Botts advised that there was no legal obligation to self-report in relation to the matters discovered. Baker Botts subsequently prepared a risk report in July 2008 regarding potential corruption in four other countries, and investigated and discovered evidence of suspected corrupt activities on at least two other occasions before 2010, but no decision was made to self-report to authorities in any country at any point.[7]

In his judgment approving the *AFWEL* DPA, Lord Justice Edis noted that there could be no criticism of Baker Botts' advice that there was no obligation to self-report, but held that 'the proper course' for the FWL board in November 2007 would have been to report the known facts to the SFO, 'not as a matter of legal duty, but as a matter of ethical corporate governance'.[8] Edis LJ went further, explaining that there is also to a 'moral duty' on all individuals (and, by implication, directors and senior managers) and firms to self-report: 'I accept that there was no legal requirement to report suspected crime to the authorities, but there is a moral duty on all citizens in this respect which extends at least equally to corporations. This failure by the board of FWL was deplorable.'[9]

The effectiveness of anti-corruption policies and procedures is inevitably linked to, and influenced by, a firm's culture. In *AFWEL*, the SFO noted that although FWEL had policies and procedures in place to prevent the type of misconduct that occurred, they were circumvented and breached on multiple occasions, which indicated 'a culture of disregard for compliance' with them.[10] Edis LJ observed that although FWEL had responded to the external lawyers' reports in 2007 and 2008 by putting in place certain measures and policy changes, these were ineffective and the offending individuals identified could continue their misconduct because, while the policies changed, they did not work because 'FWEL did not want them to'[11] and documents were instead created to conceal FWEL's engagement of agents to bribe public officials.[12] He found the evidence to be indicative of FWEL's 'widespread and high level culture of criminality'.[13]

7 ibid. at para. 26.

8 ibid. at para. 19.

9 ibid. at para. 20.

10 ibid. at para. 23.

11 ibid. at para. 24.

12 ibid. at paras. 23–25.

13 ibid. at paras. 23–25, and 29.

© Law Business Research 2021

Edis LJ emphasised that there are valuable lessons to be gleaned from the *AFWEL* DPA; not only was he clear as to what 'good' self-reporting culture involves, but also how FWEL's actions were an example of 'the culture which should be discouraged' (i.e., the 'cleansing process' of 2007–2009). He considered that the *AFWEL* DPA should therefore have the beneficial effect of improving the culture of all firms within the SFO's jurisdiction by encouraging the self-reporting of wrongdoing when they discover it, including when they find such evidence on acquisition of another entity.[14] Edis LJ also pointed out that 'a culture of self-reporting is of very substantial benefit to the interests of justice' in that it should bring to light criminal behaviour that might otherwise go undiscovered, and potentially make investigation easier, and convictions more likely.[15] This echoes Lisa Osofsky's articulation of the SFO's objective for the DPA regime nine months earlier, which she explained is to 'drive better corporate citizenship' and ensure that firms 'admit their fraud and corruption and turn their attention to cleaning house'.[16]

See Chapter 19 on whistleblowing

Financial institutions and firms' arrangements to encourage and facilitate disclosure of reportable concerns by employees or whistleblowers should allow effective escalation of reportable concerns internally to the appropriate persons or the board, and then for appropriate external escalation and reporting to appropriate bodies, including the FCA, the PRA, or the National Crime Agency (NCA) and the SFO. For regulated firms, the relevant systems and controls requirements are aligned with FCA Principle 11 and PRA Fundamental Principle 7, which oblige regulated firms to deal with their regulators openly and co-operatively, including by disclosing anything of which the regulators would reasonably expect notice, and equivalent conduct rules and obligations for senior managers under the SMCR.

The Corporate Compliance Guidance (published in January 2020) makes clear that the SFO will start assessing corporate organisations' compliance arrangements at an early stage of investigations, that deficiencies identified will not necessarily preclude an eventual DPA, provided the corporate organisation concerned is taking a 'genuinely proactive' approach to compliance. It also states that where DPAs include provisions relating to compliance programmes, the SFO is likely to require the appointment of an external monitor (at the expense of the corporate organisation) to verify that the required improvements are made.

14 ibid. at para. 35.

15 ibid. at para. 35. Edis LJ also noted that this aligned with the overriding objective in Criminal Procedure Rule 1.1 (i.e., that cases be dealt with justly, efficiently and expeditiously).

16 Lisa Osofsky, SFO Director, speech at the Cambridge International Symposium on Economic Crime 2020, 7 September 2020, available at https://www.sfo.gov.uk/2020/09/07/lisa-osofsky-speaking-at-a-presentation-hosted-by-the-cambridge-symposium-on-economic-crime/.

© Law Business Research 2021

3.3 The evolution of the link between self-reporting and a DPA

Self-reporting is a significant factor in determining a firm's chances of securing a DPA, and this connection has been the primary driver for self-reporting since the DPA regime was introduced in 2014. Yet, after seven years and a dozen DPAs, it is increasingly clear that the relationship between self-reporting and the likelihood of a DPA is not simple or binary: self-reporting in the United Kingdom does not guarantee a DPA or even leniency in sentencing (depending on whether other public interest factors are at play).

See Chapter 23 on negotiating global settlements

DPAs are now an established feature of the UK investigations landscape. Lisa Osofsky has spoken of her commitment to bringing the most complex and difficult cases of serious fraud to trial or, if in the public interest, to resolution through DPAs.[17] There are a variety of sources of useful indications as to the approaches of the SFO and the courts: in the DPAs and the judgments approving them, in cases where DPAs have not been concluded, and in the operation of prosecution guidance in ongoing investigations and negotiations. These indications are set out in more detail below, as part of the analysis of the advantages that may flow from a decision to self-report.

3.4 Obligatory self-reporting

3.4.1 Anti-money laundering and terrorist financing reporting

The sections of the United Kingdom's anti-money laundering and counter-terrorist financing legislation dealing with reporting are among the most stringent of their type in the world.

In outline, the Proceeds of Crime Act 2002 (POCA) imposes specific obligations on businesses operating in the 'regulated sector' to make suspicious activity reports (SARs) to the NCA where they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.[18] Failing to report such suspicions is an offence under section 330 POCA.

---

17 Lisa Osofsky, speech at the Cambridge International Symposium on Economic Crime 2018, Jesus College, Cambridge, 3 September 2018, available at www.sfo.gov.uk/2018/09/03/lisa-osofsky-making-the-uk-a-high-risk-country-for-fraud-bribery-and-corruption/.

18 The Proceeds of Crime Act (POCA), ss.330 and 331. On 2 June 2021, the Crown Prosecution Service (CPS) updated its guidance on prosecuting 'failure to report' cases under s.330 POCA. Before, the CPS did not charge 'failure to report' offences where there was insufficient evidence to establish that money laundering was in fact planned or undertaken. The updated guidance now states that it is possible for the CPS to charge a person under s.330 POCA as a standalone charge, even where there is insufficient evidence to establish that money laundering was planned or has taken place. By contrast, the substantive money laundering offences (ss.327–29 POCA) require a predicate offence ('criminal conduct') and the offender to know or suspect that the property represents a benefit from that criminal conduct. Given that the bar for suspicion is very low in relation to s.330 POCA, and that it is seldom clear whether money laundering is in fact occurring when the reporting obligation arises, a possible unintended consequence of this update will be a further increase in the

© Law Business Research 2021

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the MLTF Regulations) require firms that are 'relevant persons'[19] to appoint a nominated officer and to ensure that anyone who is working in the firm, handling relevant business and has the requisite suspicion in relation to money laundering will make an internal report to the nominated officer, who is then obliged to consider whether to file a SAR.[20] This means that there are (internal) reporting obligations on the individuals working in those firms. For businesses operating in the regulated sector, information triggering reporting obligations is likely to have come to them as a consequence of customer due diligence and monitoring obligations imposed by the MLTF Regulations (or their predecessors, the Money Laundering Regulations 2007).

SARs may include a request to the NCA for 'appropriate consent' to enable the reporter to do a particular act in relation to the property concerned, which might otherwise amount to the commission of a money laundering offence.[21] Such SARs have historically been referred to as 'consent SARs', although they are now referred to by the NCA as 'requests for defence against money laundering (DAML) SARs'.

There is a corresponding reporting and consent regime in relation to terrorist financing under the Terrorism Act 2000.[22] In addition, authorities may impose specific obligations on financial institutions, in particular, to report dealings with certain 'designated persons'.[23]

The relatively low threshold for making a SAR and the natural desire of businesses and the individuals within them to avoid liability (which can include potentially lengthy periods of imprisonment for individuals) means the NCA receives very substantial volumes of DAML SARs, placing a significant strain on its resources. In a review of the SAR framework completed in July 2018, the Law Commission acknowledged this, identifying that, on average, the relevant section of the NCA receives 2,000 SARs per working day, with some 100 reports seeking consent to proceed with a financial transaction.[24]

---

filing of 'defensive SARs'. See CPS: Prosecution Guidance in relation to Money Laundering Offences (last updated 2 Jun. 2021), available at https://www.cps.gov.uk/legal-guidance/money-laundering-offences.

19 A firm will be a 'relevant person' if it falls within the MLTF Regulations' definitions of (1) credit institutions, (2) financial institutions, (3) auditors, insolvency practitioners, external accountants and tax advisers, (4) independent legal professionals, (5) trust or company service providers, (6) estate agents, (7) high value dealers, and (8) casinos. MLTF Regulations, regulation 8.

20 MLTF Regulations, regulations 19 and 20.

21 POCA, ss.335 and 336.

22 The Terrorism Act 2000 (TACT), s.21A (duty for the regulated sector), s.19 (duty outside the regulated sector) and s.21ZA (consent).

23 Counter-Terrorism Act 2008, Schedule 7, para. 12, and Terrorist Asset Freezing Act 2010, s.19.

24 Law Commission's Consultation Paper, July 2018.

© Law Business Research 2021

The number of SARs submitted remains high and increases annually: the most recent statistics released by the NCA indicate that 573,085 SARs were filed between April 2019 and March 2020 (an increase of 19.78 per cent on 2018–2019) (of which 62,408 were DAML SARs, up 80.67 per cent on 2018–2019).[25] In this period, the NCA denied £172 million to suspected criminals as a result of DAML SARs, up 31 per cent on the £132 million of 2018–2019 and over three times the £52 million of 2017–18.[26] For over £100 million of the total restrained, there was no prior or existing law enforcement investigation, showing the value added by the SARs regime. The number of staff within the relevant section of the NCA has also been increasing annually.

However, for the time being at least, the volume of SARs, together with the need for the NCA to consult with other enforcement authorities potentially interested in the information (of which there will be many), typically means that the NCA is not in a position to provide consent, or to confirm whether the reporter has 'appropriate consent' to proceed (in NCA parlance, whether the reporter has a 'defence against money laundering') much before the end of the seven-working-day notice period following the filing of a SAR. This can lead to practical problems during the notice period itself and, if applicable, during the following moratorium period (which is 31 days, but may now be extended to up to 186 days on the application of investigating authorities) during which transactions will not be able to proceed. The risk of tipping off or committing other offences also leads to difficulties when communicating with customers, counterparties and others. The courts have been reluctant to interfere to accelerate this process.[27]

The United Kingdom's SARs regime is undergoing a transformation. Following a number of reviews of its effectiveness, including reports by the Financial Action Taskforce in 2018[28] and the Law Commission in 2019,[29] the UK government announced a SARs Transformation Programme to fundamentally

25 POCA, ss.335 (appropriate consent) and 336 (nominated officer consent). The NCA's most recent statistics indicate that the average turnaround time for a DAML SAR four days. See the NCA's annual SAR report, November 2020, available at https://nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020 /file.

26 These figures are not the totality of the law enforcement impact gained through SARs. Beyond the DAML regime, different agencies use SARs in many different ways (e.g., the SFO, Her Majesty's Revenue and Customs (HMRC))

27 See *National Crime Agency v. N* [2017] EWCA Civ 253; and *Lonsdale v. NatWest* [2018] EWHC 1843 (QB), for example.

28 Financial Action Task Force (FATF) Mutual Evaluation Report, 'Anti-money laundering and counter-terrorist financing measures in the United Kingdom' (1 December 2018), available at https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018-Executive-Summary.pdf. The Report found that, *inter alia*, 'the SAR regime requires a significant overhaul to improve the quality of financial intelligence available to the competent authorities', at p. 4.

29 Law Commission, 'Anti-Money Laundering: The SARs Regime Report', Law Com No. 384 (June 2019), available at https://www.lawcom.gov.uk/project/anti-money-laundering/.

© Law Business Research 2021

reform the SARs model and deliver better IT infrastructure and capabilities, enhanced feedback and a reformed UK Financial Intelligence Unit (FIU) as part of its broader five-year Economic Crime Plan in July 2019,[30] which is designed to tackle fraud and money laundering, and sets out how the UK's public and private sectors should work together to improve the response to economic crime. In May 2021, halfway into the five-year Plan, the government published its statement of progress, and noted that the Economic Crime Strategic Board had met in February 2021 to assess whether the Plan's actions remained appropriate and agreed that in certain areas – including in relation to the overhaul of the SARs regime – further momentum was needed.[31] At the time of writing, reform of the SARs regime is under way, with UK FIU staff uplift due throughout 2021 and 2022, and a new digital service for SARs reporting and analysis (including search, data visualisation and analytics) is planned for delivery by spring 2022.[32] The statement of progress hinted at possible legislative proposals for an exemption for 'ineffective DAML reporting' – there is very little information on what an exemption may entail, but it is possible the government may decline a defence to money laundering if SARs are deemed insufficiently useful or detailed.[33]

In practice, a firm's decision whether and when to file SARs to comply with reporting obligations or to secure defences to substantive offences must form part of wider strategic calculations about self-reporting. In many cases, it will be clear which enforcement authorities will be interested in investigating the circumstances that have given rise to knowledge or suspicion of (or reasonable grounds to suspect) money laundering. In such cases, it can make sense to consider providing the information set out in the SAR directly to the relevant enforcement authorities. Doing so when filing a SAR with the NCA (or soon after) can help to secure maximum credit for proactively bringing matters to the attention of the authorities and to expedite obtaining consent to proceed with a transaction. This was the course taken by Standard Bank plc in securing the United Kingdom's first DPA with the SFO in November 2015.[34] The SFO, and subsequently the court, highlighted and commended Standard Bank for reporting concerns to the SFO within weeks of the suspicious payment, and within days of filing a SAR.

The Law Commission recommended legal reforms, noting that many SARs were of 'low intelligence value and poor quality', at p. 93.

30 As set out in Actions 30–32. Policy Paper, 'Economic Crime Plan 2019 to 2022' (12 July 2019), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf.

31 As set out at Forward Delivery Plan, Action 4. Economic Crime Plan: Statement of Progress July 2019 – February 2021, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf.

32 ibid. at p. 11.

33 ibid. at p. 10.

34 *Serious Fraud Office v. Standard Bank plc* (Case No. U20150854) [2016] Lloyd's Rep FC 102.

© Law Business Research 2021

3.4.2 Mandatory sectoral reporting

A company will be subject to a variety of reporting obligations, depending on the nature of its operations, the sector in which it is involved, and the extent to which (and by which authorities) it is regulated. Each authority will have its own requirements as to the timing, format, content and process for mandatory reports. The key sectoral requirements include reporting:

- Financial sanctions breaches, to the Office for Financial Sanctions Implementation (OFSI) (on behalf of Her Majesty's Treasury).[35] Firms must inform OFSI as soon as practicable if they know, or have reasonable cause to suspect, that a person either is a target (or is acting on behalf of a target), or has committed an offence under the UK financial sanctions regime, where such information comes to the firm in the course of carrying on its business. OFSI revised its Monetary Penalty Guidance in April 2021, changing its case assessment factors and setting out explicitly that its baseline penalty matrix encourages prompt and complete voluntary disclosure.[36] Voluntary disclosures can receive a 50 per cent reduction on the baseline penalty for cases deemed 'serious', or up to 30 per cent for cases deemed 'very serious'. The absence of voluntary disclosure caps any reduction at 15 per cent for serious cases, and precludes reduction for very serious cases altogether. In the first penalty imposed since revising its Guidance, in August 2021, OFSI fined TransferGo Ltd £50,000 for breaches of the Ukraine financial sanctions regime.[37] The company did not receive any 'voluntary discount' because it had only disclosed information pertaining to some relevant transactions in response to formal OFSI information requests.
- Data security breaches under the General Data Protection Regulation. Breaches must be reported within 72 hours of becoming aware of the breach, to the Information Commissioner's Office and, in some cases, to the data subjects concerned.

35 Firms' reporting obligations under the financial sanctions regime are set out in the relevant UK regulations for each financial sanctions regime, and in chapter 3 of the Terrorist Asset-Freezing etc. Act 2010. The UK financial sanctions regime does not require regulated firms to report target matches or financial sanctions breaches to the FCA, but in practice such reports would be expected given the obligation to be open with the FCA under Principle 11 (and/or SUP15 of the FCA Handbook).

36 OFSI Guidance: Monetary penalties for breaches of financial sanctions (March 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/968229/MP_guidance_April_2021.pdf (at Chapter 4, and para. 4.9).

37 Imposition of Monetary Penalty – TransferGo Limited (5 August 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008859/050821_-_TransferGo_Penalty_Report.pdf, at para. 10.

© Law Business Research 2021

DPAs and regulatory and private agreements 3.4.3

Firms may have self-imposed reporting obligations. Reporting obligations are often built into DPAs, ongoing monitorship agreements or other agreements with regulators in relation to historic criminal or regulatory failings, for example. Where a firm has a history of such failings, it is also not uncommon for parties to key transactional and financial agreements to insist on similar reporting obligations, often tied to its mandatory or regulatory reporting obligations to particular authorities. In all cases, these obligations may have short reporting windows: firms should be familiar with them and act without undue delay.

Separately, firms may be obliged to bring the fact of an investigation, or the circumstances giving rise to it, to the attention of a host of potentially interested parties. These may include contractual counterparties, markets on which they are listed, affected customers, and insurers. It is highly likely that contractual arrangements and legal and regulatory frameworks will vary across the jurisdictions in which firms operate (e.g., applicable public procurement requirements for contracting with government entities). It is often advisable to conduct an early analysis of the potential collateral impact of historic wrongdoing and any investigation, prosecution, or negotiated outcome.

Self-reporting to the FCA and PRA 3.4.4

The FCA and, in the case of dual-regulated firms, the PRA are responsible for the conduct of firms authorised under the Financial Services and Markets Act 2000. Of particular relevance is the responsibility for ensuring that the firms and individuals regulated by it establish and maintain effective, proportionate and risk-based systems and controls to ensure that they cannot be used for the purposes of financial crime.[38]

The FCA Handbook and the PRA Rulebook contain detailed rules and guidance on their requirements in this area. These provisions supplement the overarching obligations on regulated firms and individuals to maintain an 'open and co-operative' relationship with the FCA and PRA and to 'disclose . . . appropriately anything relating to the firm of which [the relevant regulator] would reasonably expect notice'.[39] In practice, these broad principles-based requirements oblige regulated firms and individuals to notify the FCA or the PRA, or both, not only of circumstances that may amount to breaches of rules set out in the FCA Handbook or the PRA Rulebook, but also of investigations and other matters that may affect the fitness and propriety of individuals, or the ability of firms to satisfy the threshold conditions required to be authorised to carry on particular regulated activities.

38 See the FCA's Annual Report for 2020/21, available at https://www.fca.org.uk/publication/annual-reports/annual-report-2020-21.pdf.

39 PRIN 2.1.1 R, Principle 11 of the Principles for Businesses (Relations with Regulators).

© Law Business Research 2021

In recent years, the FCA has increasingly used its enforcement powers against firms and individuals for deficiencies in financial crime systems and controls. It continues to do so actively, with the most recent statistics published by the FCA indicating that it has approximately 54 such investigations open at the time of reporting.[40] It looks set to continue in this vein, having identified the area as one of its 'cross-sector priorities' in its most recent annual report. A number of enforcement cases pursued by the FCA in relation to financial crime systems and controls have been based to a significant degree on failures proactively to bring matters to the FCA's attention.[41] Looking more widely across the FCA's regulatory purview, in a number of other cases substantial penalties have been imposed on firms and individuals simply for failing to comply with obligations to notify the regulator.[42]

In a number of other areas, firms and individuals must proactively bring particular matters to the attention of the FCA, which may in due course give rise to intensified supervision, or enforcement investigations, or both. Key examples include obligations to file suspicious transaction and order reports under the Market Abuse Regulation and requirements for firms to notify the FCA (or PRA, as appropriate) of breaches of the Conduct Rules by senior managers, certified persons or other employees under the SMCR. The timescales for such notifications and the level of detail required also vary significantly depending on the circumstances.

40 FCA Enforcement annual performance report 20/21, available at https://www.fca.org.uk/data/enforcement-data-annual-report-2020-21.

41 For example, in 2015 the FCA fined The Bank of Beirut (UK) Ltd (Bank of Beirut) £2.1 million, prevented it from acquiring new customers from high-risk jurisdictions for 126 days, and fined two approved persons at the bank. The FCA noted that Bank of Beirut had also repeatedly provided the FCA with misleading information after it was required to address concerns regarding its financial crime systems and controls, including by indicating that it had completed remedial actions when it had not.

42 Recent examples: In December 2020, Charles Schwab UK Limited was fined £8.96 million for failing to adequately protect client assets, carrying out a regulated activity without permission and making a false statement to the FCA in breach of Principle 11. The final notice is available at https://www.fca.org.uk/publication/final-notices/charles-schwab-uk-limited-2020.pdf. In June 2019, the FCA fined Bank of Scotland £45.5 million for failing to disclose suspicions that fraud may have taken place within part of its corporate lending operations. The final notice is available at https://www.fca.org.uk/publication/final-notices/bank-of-scotland-2019.pdf. In 2018, Santander was fined £32.8 million for, among other things, failing to disclose information relating to certain issues with the probate and bereavement process to the FCA. The final notice is available at https://www.fca.org.uk/publication/final-notices/santander-uk-plc-2018.pdf.

© Law Business Research 2021

The FCA also acts as the UK Listing Authority, meaning that companies listed in the United Kingdom (and their directors) must behave in an open and co-operative manner,[43] which means that listed companies and their directors have to notify the FCA of potentially significant investigations.

None of the mandatory reporting obligations described above exists in a vacuum. The FCA in particular collaborates closely with other enforcement authorities, both within the United Kingdom and internationally.

Indeed, notwithstanding its ability to prosecute criminal offences, there have been several examples in recent years of cases in which it has supplied information to and otherwise coordinated its action with other authorities, including, notably, the SFO.[44] The FCA surprised the financial sector in March 2021 by launching its first criminal prosecution for offences under the Money Laundering Regulations 2007, in what is also the first prosecution of a bank (NatWest) for such offences.[45] The announcement followed a number of record fines by the FCA and HMRC for non-compliance with money laundering regulations,[46] and may mark the start of a more robust approach. NatWest pleaded guilty to the charges in October 2021 and sentencing was scheduled for December 2021 at the time of writing.

The remainder of this chapter considers self-reporting in relation to the SFO and, to the extent relevant, the FCA, in relation to financial crime issues.

---

43 FCA Handbook, LR 7.2.1 R, Listing Principle 2.

44 By way of example, the FCA did not impose a financial penalty on Tesco plc or Tesco Stores in early 2017 for engaging in market abuse, partly because Tesco Stores had entered into a DPA with the SFO, pursuant to which it would pay £128.9925 million. The FCA explained that it had also taken into account 'the exemplary co-operative approach' taken by Tesco plc and Tesco Stores with both the FCA and the SFO. See the FCA final notice, available at www.fca.org.uk/publication/final-notices/tesco-2017.pdf.

45 FCA Press Release, 'FCA starts criminal proceedings against NatWest Plc' (16 March 2021), available at https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc.

46 For example, in June 2020, the FCA fined Commerzbank London £37.8 million for inadequate AML systems and controls (final notice is available at https://www.fca.org.uk/publication/final-notices/commerzbank-ag-2020.pdf). In January 2021, HMRC fined MT Global Limited a record £23.8 million for breaches of the Money Laundering Regulations 2017, albeit under appeal at the time of writing (press release is available at https://www.gov.uk/government/news/hmrc-issues-record-238m-fine-for-money-laundering-breaches). More recently, in April 2021, HMRC announced that Irfan Ltd (MSB) had been fined £4.4 million for breaches of the Money Laundering Regulations, which has not been appealed (available at https://www.gov.uk/government/publications/businesses-not-complying-with-money-laundering-regulations-in-2018-to-2019/businesses-that-have-not-complied-with-the-regulations-and-suspensions-and-cancellations-of-registration-2020-to-2021).

© Law Business Research 2021

3.5 Voluntary self-reporting to the SFO

The SFO's decision as to whether to prosecute a corporate organisation will be governed by a combination of the Full Code Test in the Code for Crown Prosecutors,[47] the Guidance on Corporate Prosecutions,[48] (in relevant cases) the Joint Prosecution Guidance of the Director of the SFO and the Director of Public Prosecutions on the Bribery Act 2010 (the Joint UKBA Guidance),[49] and the DPA Code of Practice. Prosecutors will also follow the guidance in the relevant chapters of the SFO's internal Operational Handbook, three of which have been published in the interests of transparency since late 2019 (i.e., the Corporate Co-operation Guidance,[50] the Guidance on Evaluating Corporate Compliance Programmes (Corporate Compliance Guidance) [51] and most recently, the Guidance on Deferred Prosecution Agreements (DPA Guidance)).[52] Lisa Osofsky has explained that in combination, those sources:

> *instruct us to take into account the existence of effective compliance programmes and speedy self-reporting. It is about incentivising the private sector to co-operate in preventing crime, to be willing to report it if it occurs nonetheless, and to co-operate when we investigate and prosecute those who have transgressed.*[53]

47 The Code for Crown Prosecutors, available at www.cps.gov.uk/publication/code-crown-prosecutors.

48 The joint guidance issued by the Director of Public Prosecutions, the Director of the Serious Fraud Office and the Director of the Revenue and Customs Prosecutions Office Guidance on Corporate Prosecutions, available at www.sfo.gov.uk/?wpdmdl=1457.

49 Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions, 30 March 2011, available at www.sfo.gov.uk/?wpdmdl=1456.

50 The Corporate Co-operation Guidance was published on the SFO's website in January 2020 and is available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/evaluating-a-compliance-programme/?wpdmdl=25403&refresh=5f241d2e582d21596202286. It does not create any legally enforceable rights, expectations or liabilities.

51 The Corporate Compliance Guidance was published on the SFO's website in April 2020 and is available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/evaluating-a-compliance-programme/. It does not create any legally enforceable rights, expectations or liabilities.

52 The Guidance on Deferred Prosecutions was published on the SFO's website in October 2020 and is available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/deferred-prosecution-agreements/. It does not create any legally enforceable rights, expectations or liabilities.

53 Lisa Osofsky, SFO Director, speech at the Cambridge International Symposium on Economic Crime 2019, Jesus College, Cambridge (2 Sep. 2019), available at https://www.sfo.gov.uk/2019/09/02/cambridge-symposium-2019/.

© Law Business Research 2021

The SFO will prosecute if there is a realistic prospect of conviction on the evidence, and it is in the public interest to do so. The fact that a firm has reported itself will be a relevant consideration to the extent set out in the Guidance on Corporate Prosecutions. That guidance explains that, for a self-report to be a public interest factor tending against prosecution, it must form part of a 'genuinely proactive approach adopted by the corporate management team when the offending is brought to their notice'.[54] The SFO has long stated expressly, and has reiterated most recently in the Corporate Co-operation Guidance, that self-reporting is no guarantee that a prosecution will not follow, and that each case will turn on its own facts.[55] This is consistent with the approach of the Crown Prosecution Service (CPS) in 2018 in *R v. Skansen Interiors Ltd*,[56] the first contested case in relation to the corporate 'failure to prevent' offence under the UKBA. Skansen was prosecuted despite self-reporting to the NCA and extensive co-operation with the CPS in the ensuing criminal investigation, including by disclosing privileged material. The CPS justified its decision to prosecute rather than pursue a DPA on grounds that Skansen was a dormant company and could neither pay a fine nor comply with the terms of any DPA, and that it wanted to send a message to smaller companies as regards the importance of having effective anti-bribery and corruption procedures in place, rather than relying on 'company values' to establish proper compliance and conduct.

In appropriate cases the SFO may use its powers under proceeds of crime legislation as an alternative (or in addition) to prosecution.[57] If the SFO uses those powers, it will publish its reasons, the details of the illegal conduct and the details of the disposal.[58]

Advantages of self-reporting 3.6

Co-operation credit 3.6.1

Most firms will consider that the primary advantage of making a voluntary self-report is co-operation credit, particularly if the firm is seeking a DPA. This reflects the DPA Code, which lists co-operation as an additional public interest factor tending against prosecution.[59] As noted earlier, however, self-reporting does not secure sufficient co-operation credit to guarantee a

54 Guidance on Corporate Prosecutions, para. 32 ('Additional public interest factors against prosecution').

55 SFO's statement of policy and revised guidance on corporate self-reporting, October 2012.

56 *R v. Skansen Interiors Limited*, unreported.

57 See the Attorney General's Guidance for prosecutors and investigators on their asset recovery powers under s.2A POCA, available at www.gov.uk/guidance/asset-recovery-powers-for-prosecutors-guidance-and-background-note-2009.

58 In Scotland, where DPAs are not available, this remains the only available means of concluding bribery and fraud investigations concerning corporate organisations short of prosecution.

59 Para. 2.8.2(i).

© Law Business Research 2021

See Chapter 9 on co-operating with authorities and Chapter 23 on negotiating global settlements

DPA.[60] Self-reporting and co-operation overlap. This overlap exists because the UK's DPA regime does not draw a bold line between self-reporting and co-operation to determine whether a DPA is appropriate or any penalty reduction. Self-reporting is instead an element subsumed within co-operation, whereas the United States distinguishes between self-reporting (deserving the fullest credit) and co-operation (deserving less). Self-reporting is a less significant condition for securing a DPA in the United Kingdom – a position that has been widely criticised as undermining the regime's effectiveness.

In practice, under the UK regime, co-operation exists along a spectrum, where certain factors or steps move a firm nearer or further from the prospect of prosecution, or a negotiated outcome. The DPA Code, for example, requires co-operation to be 'genuinely proactive' and lists as examples of co-operative behaviour 'identifying relevant witnesses, disclosing their accounts and the documents shown to them . . . [and] where practicable it will involve making the witnesses available for interview when requested'.[61] Firms can find indications of what factors and steps are important on the co-operation spectrum in other guidance documents, DPAs and related judgments, many of which are considered below. Announcing the release of the DPA Guidance in October 2020, Lisa Osofsky noted: 'Over the past six years, we at the SFO have been developing our approach to negotiating and entering into DPAs, and in turn, establishing best practice. Publishing this guidance will provide further transparency on what we expect from companies looking to co-operate with us.'[62] In broad terms, three elements (i.e., timely self-reporting, proactive co-operation and implementation of effective compliance remediation) will determine, to a greater or lesser degree, the level of co-operation credit a firm may receive.

The Joint Guidance on Corporate Prosecutions lists co-operation as a factor tending against prosecution, but instructs prosecutors first to establish whether the firm has provided sufficient information about its operations 'to assess whether the company has been proactively compliant' including 'making witnesses available and disclosure of the details of any internal investigation'.[63]

60 See, for example, *R v. Skansen Interiors Limited*, unreported. It is important to differentiate *Skansen*, however, as it was prosecuted by the CPS and was dormant. The SFO may be more inclined to pursue a DPA, particularly in circumstances where parent entities are willing to pay fines or provide appropriate undertakings, as indicated by the three DPAs agreed with the SFO in July 2021 (i.e., the *AFWEL* DPA, and the DPAs agreed with two anonymous companies and subject to reporting restrictions at the time of writing).

61 ibid.

62 SFO Press Release (23 October 2020), available at https://www.sfo.gov.uk/2020/10/23/serious-fraud-office-releases-guidance-on-deferred-prosecution-agreements/.

63 Guidance on Corporate Prosecutions, p. 8.

© Law Business Research 2021

In approving DPAs between the SFO and Standard Bank, Sarclad Ltd[64] and Rolls-Royce, Sir Brian Leveson spoke positively of the co-operative stance adopted by each of those firms, as did Mr Justice William Davis, approving the DPAs agreed with Serco and Güralp, and Dame Victoria Sharp, approving the DPA with Airbus.

The SFO's Corporate Co-operation Guidance,[65] 'does not seek to set out exhaustively what will be required in order for a corporate organisation to be considered as genuinely co-operative', since 'there will be dialogue in every case about what will be expected of the corporate organisation concerned'.[66] It notes in general terms that:

> *Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrong-doing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.*

Non-exhaustive as it declares itself to be, it does add some detail (and confirm previous public statements) as to what is good practice and lists steps firms should take, including regarding the preservation and production of relevant digital and hard-copy information; evidence of financial records and analysis (to 'show relevant money flows'); the provision of industry and background information (including about other actors in the market and whether any other government agencies are aware); and taking witness evidence (including an expectation that co-operating firms will waive privilege over witness accounts).

However, to understand the effect of any such co-operation, companies and practitioners still must look to the DPA Code, which sets out prosecutors' expectations regarding self-reporting. In deciding whether a DPA is appropriate, along with other factors relating to the nature and seriousness of the offending, prosecutors must evaluate whether the firm has been 'genuinely proactive' in its approach.[67] Proactiveness is measured by reference to factors including the timing of the self-report, and how comprehensive, relevant and useful the material is (particularly as regards any potential action against individuals).

64 *Serious Fraud Office v. XYZ Limited* (now known to be Sarclad Ltd) (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509.

65 SFO Operational Handbook, Corporate Co-operation Guidance, p. 1, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

66 As part of the SFO's Operational Handbook, it expressly states that it does not create legally enforceable rights, expectations or liabilities.

67 DPA Code, para. 2.8.2.

© Law Business Research 2021

3.6.1.1 Timing

The DPA Code[68] the SFO's Corporate Co-operation Guidance,[69] and the DPA Guidance make it clear that firms wishing to obtain as much co-operation credit as possible should not wait until they have carried out their own detailed internal investigation before self-reporting concerns about possible wrongdoing.[70] The Corporate Co-operation Guidance and DPA Guidance reiterate previous general indications that self-reporting should occur 'within a reasonable time' of the firm becoming aware of the relevant matters. What is clear is that prosecutors expect to receive an initial notification of circumstances giving rise to concerns that criminal wrongdoing may have occurred. They do not expect or wish to receive a completed investigation report. As is set out in the DPA Code, the Corporate Co-operation Guidance and the DPA Guidance, they expect to be involved in the investigation at the planning stage and certainly before any witness interviews are conducted.[71] In cases where firms discover evidence of significant historic wrongdoing that is not already known to prosecutors and may suitably be resolved through a DPA, they should consider making an initial notification to the SFO (or CPS, if appropriate) at the same time as they file suspicious activity reports (SARs) or other statutory reports (in the United Kingdom or abroad).

The timing of a self-report relative to any details entering the public domain is particularly important. The DPA Guidance specifically highlights that self-reporting be made 'voluntarily, that is without the threat of imminent disclosure by a third party or compulsion'.[72] That it was still possible for the SFO to conclude a DPA with Rolls-Royce in 2017 despite some details of wrongdoing already being known to the SFO illustrates that this is just one factor informing a prosecutor's approach and does not by itself determine whether a

68 DPA Code, para. 2.8.1(v): 'Failure to notify the wrongdoing within a reasonable time of the offending conduct coming to light.'

69 SFO Operational Handbook, Corporate Co-operation Guidance, at p. 1 ('Co-operation means . . . reporting [suspected wrongdoing] to the SFO within a reasonable time of the suspicions coming to light.'), available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

70 The DPA Code used the word 'notified' in this context, which replaced the word 'reported' in the original draft of the DPA Code. Although (perhaps because it was not the subject of a consultation exercise before its publication in August 2019) the same distinction between 'reporting' and 'notifying' is not drawn in the Corporate Co-operation Guidance, the message prosecutors are seeking to convey is the same. The DPA Guidance uses the verb 'notify'.

71 DPA Code, para. 2.9.2; SFO Operational Handbook, Corporate Co-operation Guidance, at p. 4: 'To avoid prejudice to the investigation, consult in a timely way with the SFO before interviewing potential witnesses or suspects, taking personnel/HR actions or taking other overt steps.', available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

72 SFO Operational Handbook, DPA Guidance, 'Self-Reporting' section.

© Law Business Research 2021

DPA will follow.[73] However, Sir Brian Leveson, then President of the Queen's Bench Division, noted that *Rolls-Royce* was anomalous in this regard, and that for Rolls-Royce to obtain credit for self-reporting in DPA negotiations it was necessary for the company to provide 'extraordinary' co-operation and to notify the SFO of matters 'of a different order' to those it would otherwise have known.[74] Absent such extraordinary co-operation and disclosure, it is clear that a failure to notify the SFO of matters before they become public (or before negative headlines are threatened or imminent) will jeopardise the prospects of successfully negotiating a DPA.

The DPA Code's focus on proactive and timely self-reports is illustrated by the January 2020 DPA agreed with Airbus SE.[75] Airbus received a degree of 'co-operation credit' for having initially reported corruption concerns to a UK government body that Airbus knew was required to report onward to the SFO, effectively forcing Airbus to self-report. Airbus received credit, despite, as Dame Victoria Sharp pointed out in approving the DPA, 'the true catalyst' for the self-report being the 'watchfulness' of the government body rather than Airbus itself.[76] Airbus had initially identified concerns about business partners from late 2013 and took steps to address them from early 2014. In April 2015, the UK government body from which Airbus obtained export credit financing– UK Export Finance (UKEF) – queried the lack of information in certain declarations required of Airbus as part of UKEF anti-bribery due diligence. Crucially, it notified Airbus at the time of its queries that it had to report any suspicions of corruption to the SFO. This prompted Airbus to investigate and make fuller disclosures to UKEF in January and March 2016. Having received Airbus' fulsome disclosure, UKEF informed Airbus that it would notify the SFO and that its strong preference was for Airbus also to do so. Both UKEF and Airbus reported to the SFO on 1 April 2016, and Airbus met with the SFO a week later. Technically, therefore, Airbus did not itself decide whether or when to self-report – UKEF made those decisions for it.

Lord Justice Edis was at pains to emphasise the significance of the timing of a self-report in his judgment approving the *AFWEL* DPA in March 2021. Edis LJ considered that failing to self-report at the time the facts were discovered was an aggravating factor because so much time had been able to pass, not only since the first Baker Botts report in 2007, but also since the offending itself occurred. The Baker Botts reports were historical and related to conduct some time before. Edis LJ noted that this 'means that it may be more difficult to

73 As noted in the Corporate Co-operation Guidance: 'Each case will turn on its own facts. In discussing co-operation with an organisation, the SFO will make clear that the nature and extent of the organisation's co-operation is one of many factors that the SFO will take into consideration when determining an appropriate resolution to its investigation.' ibid., p. 1.

74 *Serious Fraud Office v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc.* (Case No. U20170036) [2017] Lloyd's Rep FC 249, paras. 21 and 22.

75 *Serious Fraud Office v Airbus SE* [2020] 1 WLUK 435.

76 ibid., at para. 71.

© Law Business Research 2021

investigate and prosecute individual offenders now'.[77] Significantly, offending only began in Brazil three years after the board had received the external lawyers' reports of similar misconduct in other countries in 2007 and 2008. Edis LJ considered that self-reporting in 2007–2008 might have prevented the spread of misconduct to other countries, but conceded that given 'that corruption appears to have been endemic then and at a very high level, it may be doubted that this would ever have happened'.[78]

3.6.1.2 Continuing co-operation

It is not only the timing of an initial notification that matters. To demonstrate the requisite level of co-operation for a DPA to be appropriate, firms must also remain appropriately engaged with prosecutors as investigations progress. The DPA with G4S Care and Justice (UK) Limited (G4S) in July 2020 provides an illustration.[79] In that case, the company and its representatives sustained the possibility of a DPA for approximately six years after its initial notification to the SFO, only opting to increase levels of active co-operation in October 2019, with the concerted aim of concluding the DPA. Approving that DPA, Mr Justice William Davis made clear that 'initial reluctance' in co-operation would not preclude a DPA, but is relevant to the reduction to be applied to the financial penalty element, which, for G4S, was set at 40 per cent rather than 50 per cent as in all other UK DPAs to date other than that agreed with Standard Bank.

Similarly, as described above, in approving the *Airbus* DPA, Dame Victoria Sharp found that despite 'what might be described as a slow start' (i.e., corruption concerns were apparent from late 2014 but disclosures were only made in early 2016, first to UKEF and then to the SFO), Airbus had thereafter 'co-operated with the prosecuting authorities conducting the investigations to the fullest extent possible'. Sharp P attached particular weight to the fact that Airbus accepted from the earliest stage in its dealings with the SFO that the UKBA gave the SFO extended extraterritorial powers (and cause for interest) in relation to conduct that had occurred almost exclusively overseas, which she acknowledged was 'an unprecedented step' for a company domiciled in France and the Netherlands.[80] Airbus' initial delays in providing full co-operation were not considered sufficiently substantial to merit any reduction to the discount applied to the financial penalty element of the DPA, however.[81] As Sharp P noted, 'there is no necessary bright line between self-reporting and co-operation'.[82]

77 ibid. at para. 20.

78 ibid. at paras. 18, 20 and 35.

79 *Serious Fraud Office v. G4S Care and Justice (UK) Limited* [2020] 7 WLUK 303.

80 ibid., at para. 72.

81 *Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435 at para. 69.

82 ibid., at para. 68.

© Law Business Research 2021

G4S and Airbus remained on the correct side of the lines around the timing of (and rationale behind) initial notification and the levels of subsequent co-operation. The SFO considered that both lines had been crossed by Sweett Group plc, however, which was prosecuted in December 2015 for failure to prevent bribery under the UKBA. Sweett had self-reported on learning that a newspaper intended to publish allegations of involvement in bribery in connection with Middle Eastern construction consultancy agreements. As noted above, the recent DPA Guidance specifically highlights that self-reporting due to 'imminent threat' of disclosure undermines the 'voluntary' quality of the report. Although informal discussions about DPAs did commence at one stage, Sweett was deemed to have been unco-operative for much of the investigation, leading ultimately to conviction and the imposition of a fine of £2.25 million in February 2016.

Waiving privilege 3.6.1.3

The Corporate Co-operation Guidance and DPA Guidance are clear that firms cannot be compelled to waive privilege over relevant materials or be penalised for not doing so. In practice, maintaining privilege will effectively be a factor tending in favour of prosecution. For now, the guidance has to be read together with the body of case law relating to DPAs in the United Kingdom. In these cases, 'genuine and proactive' co-operation has manifested itself largely through pragmatic decisions by firms to waive privilege on a limited basis and to make material available voluntarily (i.e., without requiring the SFO to use powers of compulsion, although the Corporate Co-operation Guidance and DPA Guidance confirm if the SFO perceives a need to use its powers of compulsion, it will not necessarily mean that the firm concerned is not suitably co-operating). Most recently, for example, Airline Services Limited provided access under a limited waiver of privilege not only to material from its internal investigation into the conduct and contracts forming the subject of its self-report and DPA, but also in relation to an earlier internal investigation into conduct involving a different agent and related contracting arrangements.[83] G4S also provided access to all interviews conducted by its lawyers and accountants under a limited waiver of privilege. In all cases it has been crucial to show a clear separation from the individuals alleged to have been involved in wrongdoing and a commitment to providing material for use in prosecuting any culpable individuals. The provision of such material has not yet contributed to the successful prosecution of any individual for the conduct in respect of which the corporate entity entered into a DPA, however.[84]

83 *Serious Fraud Office v. Airline Services Limited* (Case No. U20201913, October 2020) at para. 72, available at https://www.sfo.gov.uk/2020/10/30/sfo-enters-into-deferred-prosecution-agreement-with-airline-services-limited/.

84 See, e.g., the discontinuation of proceedings against former senior executives of Tesco Stores Limited in late 2018 (https://www.sfo.gov.uk/2018/12/06/no-case-to-answer-ruling-in-case-against-former-tesco-executives/), the acquittal in July 2019 of employees of Sarclad Limited

© Law Business Research 2021

3.6.2 Leniency or reductions at the penalty stage

Self-reporting and subsequent co-operation are also relevant at later stages in the UK criminal justice process. The Sentencing Council's Definitive Guideline[85] (effective from 1 October 2014 in relation to the sentencing of corporates for fraud, bribery and money laundering offences and considered in setting financial penalties under a DPA), takes into account a firm's culture in the event of a conviction.[86] The Guideline sets out steps to assist courts in determining the appropriate fine. The first is to establish the harm caused by the offending. For example, for a bribery offence, the starting point for the calculation is the 'harm figure' – the gross profit from the contract obtained. Once a harm figure has been determined, the court establishes the 'culpability' factor by reference to a scale in the Definitive Guideline (from 'A' for high culpability down to 'C' for lesser culpability). Each level of culpability has attached to it a range of multipliers to apply to the harm figure. In determining exactly which multiplier to apply, the court must take into account many factors. One is co-operation with the investigation (which includes and is not separate from, self-reporting), which the Definitive Guideline lists as reducing the culpability multiplier.

The co-operation reductions applied by the SFO to date have been significantly more generous than those of its US counterpart. The UK legislation requires any financial penalty forming part of a DPA to be broadly comparable to the fine a court would have imposed following a guilty plea.[87] In the very first DPA (with Standard Bank plc) in 2015, the SFO and court had followed the legislation and the DPA Code to the letter by providing a discount of one third – equivalent to the reduction ordinarily afforded a guilty plea at the earliest opportunity under the existing sentencing principles and guidelines. Ever since, however – presumably on the basis that incentivising self-reporting and co-operation would require companies to receive more credit than they might ordinarily get in return for a simple (early) guilty plea – in all but one of the DPAs in which the SFO has applied a co-operation discount to date, the discount has been set at 50 per cent.[88]

(which was anonymised as 'XYZ' when the DPA was entered into with the company, at which point reporting restrictions were in place due to the continuing proceedings against three employees (https://www.sfo.gov.uk/2019/07/16/three-individuals-acquitted-as-sfo-confirms-dpa-with-sarclad/)) and the acquittal in December 2019 of three individuals formerly associated with Güralp Systems Limited (https://www.sfo.gov.uk/cases/guralp-systems-ltd/).

85 Sentencing Council's Definitive Guideline 'Corporate Offenders: Fraud, Bribery and Money Laundering', available at www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-bribery-and-money-laundering-offences-Definitive-guideline2.pdf.

86 A culture of wilful disregard for the commission of offences will lead to a corporate being placed at the most culpable end of the spectrum and facing the heaviest fines.

87 Crime and Courts Act 2013, Schedule 17, para. 5(4).

88 It is not known whether a discount applied to the SFO's two most recent DPAs agreed with two anonymous companies in July 2021. At the time of writing, the DPAs, statement of facts,

© Law Business Research 2021

The SFO has drawn criticism for undermining the effectiveness of the United Kingdom's DPA regime with its over-generous approach to co-operation credit in penalty reductions. Shortly after the Airbus DPA was approved in February 2020, for example, Transparency International and Spotlight on Corruption called in an open letter for Lisa Osofsky to review the regime (in conjunction with the Attorney General's Office and the CPS) and urged the SFO to follow the US approach to the distinction between self-reporting and co-operation, so that self-reporting would be a more significant condition for securing a DPA.[89] The letter's argument that the absence of this distinction creates perverse incentives for firms to wait until after wrongdoing has been discovered by authorities, and then make a virtue of co-operation, is neither novel nor isolated.

Arguably, financial services firms have less scope for truly voluntary self-reporting because, Principle 11 requires disclosure of 'anything relating to the firm of which that regulator would reasonably expect notice'[90] and the SMCR imposes corresponding obligations on senior managers.[91] The FCA sets out a non-exhaustive list of factors relevant to determining whether to issue a financial penalty or public censure in its Decision Procedure and Penalties Manual (DEPP), which includes 'how quickly, effectively and completely the person brought the breach to the attention of the FCA or another relevant regulatory authority'.[92] If the FCA decides to take action against a firm, DEPP operates similarly to the Definitive Guideline in setting an appropriate level, noting that 'the conduct of the firm in bringing (or failing to bring) quickly, effectively and completely the breach to the FCA's attention' is one of the factors for increasing or decreasing the fine.[93]

Demonstrating culture and the strength of systems and controls 3.6.3

Effective self-reporting indicates a good corporate culture. Firms that have taken the necessary steps to institute a good culture supported by robust systems and controls will expect that any matters involving wrongdoing would be quickly reported internally via their whistleblowing procedures and escalated, reported to the relevant authorities, or both, as appropriate. Further, self-reporting can be used as part of a firm's 'reasonable procedures' defence if charged with one of the corporate failure-to-prevent offences, such as the failure to prevent bribery

---

and judgment were subject to a reporting restriction order, and not published. The SFO's announcement is available at https://www.sfo.gov.uk/2021/07/20/sfo-secures-two-dpas-with-companies-for-bribery-act-offences/.

89 Open Letter to the Director of the Serious Fraud Office, 'Strengthening the UK's Deferred Prosecution Agreement Regime', https://www.transparency.org.uk/publications/airbus-uk-deferred-prosecution-agreement-dpa-bribery-sfo-lisa-osofsky/.

90 FCA Handbook, PRIN 2.1.1 R. An equivalent obligation to notify the PRA is set out in Fundamental Rule 7.

91 Senior Manager Conduct Rule 4 is set out in the FCA Handbook at COCON 2.2.4R.

92 FCA Handbook, DEPP 6.2.1 (2)(a).

93 ibid., DEPP 6.5A.3 (2)(a).

© Law Business Research 2021

under section 7 of the UKBA, or the failure to prevent the facilitation of UK or foreign tax evasion under the Criminal Finances Act.[94]

Conversely, a regulated firm's failure to identify and self-report wrongdoing could indicate a breach of the FCA's requirements for such firms to:

> *establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.*[95]

3.6.4 Information control

Firms often think that choosing to self-report will enable them to retain control over the information that they disclose. In practice, however, the SFO and FCA's insistence on effective self-reporting means that firms will have to provide as complete an account as possible of the wrongdoing concerned, and hand over particular investigative work-products (or categories of work-product) already created. Public companies will also have to give careful consideration to their obligations to make market announcements.

See Chapter 38 on publicity

Given the stance adopted by the FCA and SFO, perhaps the only true benefit to self-reporting is that the firm has some control over the timetable (as compared, for instance, with a dawn raid) and is therefore able (having taken advice on any market abuse risks) to notify key stakeholders of the self-report and to prepare an appropriate media strategy.

3.7 Risks in self-reporting

It should be clear that self-reporting in the United Kingdom does not guarantee a DPA or even leniency in sentencing. In most cases, a firm will only be able to gauge its DPA prospects relatively late in a process during which it will usually have provided a significant amount of information, documents, investigation reports and even witnesses for interview, having possibly waived privilege.[96] The *G4S* DPA of July 2020 indicates that in some circumstances a firm may postpone its decision about whether to engage more fully until a relatively late stage in the investigation. That said, it would be risky for firms to regard *G4S*, which was rooted in a very particular factual context, as a guide to the approach prosecutors may take in future. The relevant chapters of the SFO's Operational Handbook contain express warnings to firms that none of their provisions concerning its

94 HMRC Guidance: Tell HMRC your organisation failed to prevent the facilitation of tax evasion, available at https://www.gov.uk/guidance/tell-hmrc-your-organisation-failed-to-prevent-the-facilitation-of-tax-evasion#how-self-reporting-could-benefit-your-organisation.

95 FCA Handbook, SYSC 6.1.1R.

96 In the United Kingdom, court approval is required for a DPA, which means that even if the SFO recommends a DPA after extensive co-operation, the court may reject it.

© Law Business Research 2021

expectations around self-reporting and cooperation are legally binding and should not be taken to create any rights, liabilities or expectations. In a slightly different context, *Soma Oil & Gas Limited v. Director of the Serious Fraud Office*[97] provides an illustration of the expense, difficulty and disruption associated with seeking to force the SFO to bring about a conclusion to an investigation. Firms therefore need to evaluate the risks and costs inherent in making self-reports carefully. Some key risks and practical considerations are set out below.

Interest and potential investigation in other jurisdictions 3.7.1

There is always a risk of contagion: it is the nature of complex bribery, fraud and corruption that it crosses borders and can implicate authorities in multiple jurisdictions. Self-reporting to a regulator in one jurisdiction may draw the attention of other regulators, domestically or abroad. The benefits and risks of reporting are seldom consistent or certain across jurisdictions, since procedures, techniques or demands in conducting their investigations and taking enforcement action inevitably differ.

Increasingly, regulators are sharing information and seeking to collaborate in enforcement actions. As long ago as 2010, the US Department of Justice and the SFO worked together in investigating BAE Systems plc,[98] and such co-operation has since become routine. International co-operation often goes beyond formal mutual legal assistance requests, to encompass informal intelligence sharing (sometimes in advance of formal investigation in any jurisdiction), coordination or division of responsibility on issues for enforcement, and even formal programmes by which to enhance understanding and assist with capacity or resourcing. This has included (and continues to include) SFO secondments by prosecutors from US and Singaporean authorities and an expanding list of memoranda of understanding with overseas counterparts. Lisa Osofsky confirmed the SFO's commitment to ongoing international co-operation in a speech in April 2019[99] and international co-operation routinely features as a strategic objective in the SFO's Annual Report.[100] The Airbus global settlement incorporating DPAs negotiated by the SFO and the US Department of Justice and an analogous *convention judiciaire d'intérêt public* (CJIP) with the France's financial crime prosecutor, the Parquet National Financier in France is the most significant example of such co-ordinated action to date.

97 *Soma Oil & Gas Limited v. Director of the Serious Fraud Office* [2016] EWHC 2471 (Admin).

98 See the US Department of Justice's expression of gratitude to the SFO for its assistance in its press release, March 2010, available at www.justice.gov/opa/pr/bae-systems-plc-pleads-guilty-and-ordered-pay-400-million-criminal-fine.

99 Lisa Osofsky, Director of the SFO, speech at the Royal United Services Institute, 3 April 2019, available at https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/.

100 For example, see the SFO's most recent Annual Report for 2020/2021 (published 9 Jul. 2021), available at https://www.sfo.gov.uk/download/annual-report-and-accounts-2020-2021, at p. 12.

© Law Business Research 2021

While there are legal limits to the extent of information sharing and collaboration between authorities, firms need to be strategic in their conduct across all countries. For example, US law significantly limits the use (or derivative use) of defendants' foreign compelled testimony in US criminal proceedings against them.[101] The UK provision of evidence or interview testimony is commonly compelled in the United Kingdom,[102] which means that there is a real risk that firms may fall foul of those limits (even inadvertently, as part of routine updates or reports on progress or developments in parallel investigations) and negate any co-operation credit otherwise achieved in the United States.

3.7.2 Privilege and authorities' involvement in the internal investigation

3.7.2.1 Legal advice in relation to internal investigations

A key concern for all firms considering and investigating suspicions or allegations of wrongdoing is to establish clearly at the outset that its board, or any committee with oversight of internal investigations, is authorised to seek and receive legal advice in relation to the investigation to ensure that updates to these bodies and related documents will be protected by legal professional privilege.

See Chapter 35 on privilege

3.7.2.2 Material generated during internal investigations

A significant concern in the context of internal investigations centres on the material generated during an internal investigation, including any investigation work and work-product that may have preceded the self-report. This material typically includes interview notes and summaries of key documents and issues.

The UK authorities are adamant that to self-report in any meaningful sense, firms must provide sufficiently detailed information about the wrongdoing. The SFO states: 'All supporting evidence including, but not limited to emails, banking evidence and witness accounts, must be provided to the SFO's Intelligence Unit as part of the self-reporting process.'[103] A key question when considering a self-report is thus whether it is prepared to disclose its full interview notes, the privileged status of which has been subject to heated debate in the United Kingdom in recent years.

---

101 *United States v. Allen*, 864 F.3d 64 (2d Cir. 2017), reh'g en banc denied, No. 16-898 (2d Cir. 9 Nov. 2017).

102 For example, the SFO may compel a person to attend an interview with SFO staff to answer questions or otherwise furnish information pursuant to s.2 of the Criminal Justice Act 1987. Similarly, pursuant to s.171 of the Financial Services and Markets Act 2000, the FCA may require persons under investigation to attend an interview with an investigator to answer questions, or otherwise provide information as requested. Other enforcement agencies, including HMRC, the Competition and Markets Authority and the NCA have similar powers to compel information under various statutes. Suspects in criminal investigations must be interviewed under caution pursuant to the Police and Criminal Evidence Act.

103 www.sfo.gov.uk/publications/guidance-policy-and-protocols/corporate-self-reporting/.

© Law Business Research 2021

See Chapter 35 on privilege; Section 35.4.2

The September 2018 Court of Appeal ruling in *ENRC* is the key case in this context.[104] The Court reiterated the established principle that litigation privilege may be claimed over documents created when litigation was in 'reasonable contemplation' and for the purposes of that litigation. Such determinations are necessarily fact-specific. Notably, the Court held that, on the *ENRC* facts, the interview notes generated during the course of its internal investigation were subject to litigation privilege on the basis that (1) they had been brought into existence after ENRC's external counsel (who were conducting an investigation) had advised that there was a real and serious risk of law enforcement and regulatory intervention, including criminal prosecution, and (2) the notes were, in the Court of Appeal's estimation, drafted to assist any future defence of such proceedings.

If a further illustration of the potential complexities and follow-on implications of DPAs were needed, it is provided by *Omers Administration Corporation and others v. Tesco plc*.[105] In a judgment handed down in January 2019 in civil proceedings pursued by investors for losses they claim resulted from the conduct forming the basis of the DPA agreed between the SFO and Tesco Stores Limited, Mr Justice Hildyard ordered disclosure of documents in the possession or control of Tesco plc. These included some documents provided to it by the SFO, which had been obtained from third parties through the use of the SFO's compulsory powers under section 2 of the Criminal Justice Act 1987, and transcripts of interviews with, and witness statements of, third parties. The conflict between Tesco plc's obligations to keep these documents confidential pursuant to an undertaking provided to the SFO as part of the DPA negotiation process, and its disclosure obligations in the follow-on litigation pursued by investors under the Financial Services and Markets Act 2000, generated substantial ancillary litigation and a costly and involved process of seeking representations from third parties. An appeal in relation to aspects of that decision is pending at the time of writing. However, the proceedings serve as a reminder that although a DPA may avoid the need for protracted criminal proceedings, it provides no guarantee of finality in respect of (and indeed may provide oxygen for) associated civil (or regulatory) proceedings.

Waiving privilege 3.7.2.3

The SFO has maintained for some time that firms wishing to co-operate with the SFO need to give serious consideration to waiving privilege, and that it is ready to challenge any overly broad claims to privilege. The Corporate Co-operation Guidance reinforces that approach. It notes that a firm's claim to privilege must be properly established, that any claim should be supported by independent counsel, and that the Court of Appeal ruling in *ENRC* 'has not

104 *Director of the Serious Fraud Office v. Eurasian Natural Resources Limited (Law Society intervening)* [2018] EWCA Civ 2006.

105 *Omers Administration Corporation and others v. Tesco plc* [2019] EWHC 109 (Ch).

© Law Business Research 2021

ruled out a court's consideration of the effect of an organisation's non-waiver over witness accounts in determining whether a proposed DPA is in the interests of justice'.[106]

Following *ENRC*, it is open to any company that has conducted an initial investigation and received clear legal advice that the information unearthed may amount to a criminal offence or a regulatory failing[107] to claim that any material generated in the course of that initial internal investigation will be subject to litigation privilege. However, the Court of Appeal's judgment in *ENRC* made it clear that nothing it said about privilege should adversely impact the DPA regime and, furthermore, that maintaining claims to privilege may adversely affect prospects of obtaining a DPA.[108] The Court also noted: 'Had the court been asked to approve a DPA between ENRC and the SFO, the company's failure to make good on its promises to be full and frank would undoubtedly have counted against it.'[109]

See Chapter 36 on privilege

In deciding whether to acquiesce in providing witness accounts and other privileged materials, a company will need clear advice as to the risks involved in waiving litigation privilege, even on a limited basis, at such an early stage, particularly before it is clear whether a settled resolution is likely and especially where multiple authorities may be involved. The shield of litigation privilege is clearly of paramount importance to any firm defending criminal or regulatory enforcement proceedings where, very commonly, civil litigants will be waiting in the wings and in jurisdictions such as the United States, where the concept of limited waiver does not exist.

3.7.2.4 Involvement of authorities in internal investigation

Having ensured that the internal investigation is suitably established for privilege purposes, another critical concern for any firm will be the likelihood of potential involvement in, or loss of control of the scope, timing and conduct of, its own investigation. The former Director of the SFO, Sir David Green QC, made it clear that the SFO might specify particular areas or issues to be included in the firm's investigation, how the investigation ought to be conducted in relation to particular issues or persons, and to provide updates to the SFO, usually within agreed time frames.[110] He explained the SFO's influence or imposition into internal investigations as being necessary to avoid

106 SFO Operational Handbook, Corporate Co-operation Guidance, p. 1 at note 5, citing *The Director of the Serious Fraud Office v. ENRC* [2018] EWCA Civ 2006 at para. 117, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

107 Indeed it is not clear on what other basis such a company would self-report.

108 *Director of the Serious Fraud Office v. Eurasian Natural Resources Limited (Law Society intervening)* [2018] EWCA Civ 2006, at paras. 115 to 117.

109 ibid.

110 Sir David Green QC, former SFO Director, speech at GIR Roundtable Discussion on Corporate Internal Investigations, 27 July 2015.

© Law Business Research 2021

'churning up the crime scene' and compromising the SFO's own investigation. This, again, is reinforced in the Corporate Co-operation Guidance. The judgment released in relation to the *Airbus* DPA provides particularly clear confirmation that, in addition to watching closely how internal investigations are conducted, the SFO will 'interrogate and validate the narrative' provided by self-reporting firms by conducting its own investigation.[111]

Similar sentiment was expressed by Mark Steward, the FCA's Head of Enforcement, who referred to 'the crime scene being trampled over'.

Impact on witness interviews 3.7.3

In addition to influencing the scope of an internal investigation, UK authorities may also influence a firm's ability to conduct witness interviews after self-reporting, whether by prohibiting the firm from conducting interviews with certain individuals, or by requiring the firm to delay them until the authority has conducted its own interviews. In *Rolls-Royce*, for example, Sir Brian Leveson noted that when the SFO commenced its own investigation, Rolls-Royce had not only provided access to its internal investigations and interview notes (by a limited waiver of its claims for legal professional privilege over them), but also deferred its own interviews until after the SFO had done so.

Scrutiny, including potential monitoring obligations 3.7.4

A DPA or settled resolution will always include a number of non-financial terms and conditions. While these will often be fact-dependent and tailored to the wrongdoing involved and the state of the firm's remediation at the point of agreement, the DPA Code includes a list of terms that may be agreed as part of a DPA, including requirements for putting in place a robust compliance or monitoring programme, or both, which may include the appointment of an independent monitor.[112]

While the imposition of a corporate monitor is not compulsory, the DPA Code provides lengthy guidance as to monitors' roles and appointment, and notes that the imposition of a monitor 'must always be fair, reasonable and proportionate'.[113] Where a monitor is required, the costs to the firm can be significant. Not only will the firm have to pay the monitor's fees, but it will also have to pay the costs associated with the selection, appointment and reasonable 'monitoring' costs of the prosecutor during the monitoring period. There are indirect or non-financial costs, too. The monitor must be given complete access to all relevant aspects of the firm's business and the firm will need to allocate resources to ensure that the monitor is provided with the information and co-operation required and to establish the systems and controls necessary to effect the remediation agreed with the regulator.

111 *Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435, at para. 37.

112 DPA Code, para. 7.10(iii).

113 ibid., paras. 7.11 to 7.22.

© Law Business Research 2021

These costs have attracted a degree of judicial and corporate scepticism and criticism in the United Kingdom and the United States. Such criticism notwithstanding, the appointment of a monitor (in one form or another) is likely to feature regularly in DPAs in the future, as had previously been the case in civil recovery orders[114] or criminal court orders,[115] which were the SFO's preferred means of imposing monitorships before the introduction of the DPA regime provided it with a statutory basis for doing so.

However, the DPAs concluded to date surely illustrate that a distinctive feature of the UK DPA framework is its flexibility; prosecutors negotiating and judges approving DPAs in the United Kingdom have significant discretion to decide the nature and extent of any monitoring and reporting arrangements that may be necessary or desirable as part of the remediation elements of DPAs. Viewing the Corporate Co-operation Guidance together with the *G4S* settlement's inclusion of a more extensive role for a third party effectively acting as a monitor, it may be that Lisa Osofsky is bringing her previous experiences as a monitor in private practice and as a US investigator and prosecutor to bear on her role as Director of the SFO.

3.8 Practical considerations, step by step

3.8.1 Reaching the decision

Sometimes the decision to self-report may be clear-cut or the only sensible option (particularly where a whistleblower has made serious allegations). More often, however, it will be necessary to conduct an internal investigation to test the information underlying the concerns and to ensure that any report made to authorities is as complete and accurate as possible. How long this takes will depend on a range of factors, including where and when the alleged conduct took place, the number of individuals allegedly involved, and the availability of relevant documents and individuals for interview. It is critical for the decision to self-report to be taken by directors who are independent of the underlying events or issues, in conjunction with appropriate legal advisers, and suitably documented. An essential first step is immediately preserving all relevant documents, and ensuring that the investigation is carefully scoped and proceeds expeditiously.

There is no one 'correct' approach to investigating disclosures, allegations or whistleblowers' reports. What is necessary and appropriate will vary significantly depending on factors including the jurisdictions, personnel and business areas implicated. The following key principles may, however, help firms to

114 For example, the civil recovery orders between the SFO and Balfour Beatty plc in October 2008; Macmillan Publishers Ltd in July 2011; and Oxford Publishing Ltd in July 2012.

115 For example, in relation to Mabey & Johnson in September 2009, as well as Innospec Ltd in March 2010: see https://star.worldbank.org/corruption-cases/sites/corruption-cases/files/documents/arw/Mabey_Johnson_UK_SFO_Press_Release_Sentencing_Sep_25_2009.pdf and https://www.sfo.gov.uk/cases/innospec-ltd/, respectively.

© Law Business Research 2021

respond decisively and consistently to disclosures of alleged misconduct, and to protect their interests when they do.

Clear communication 3.8.1.1

Clear communication underpins a successful response to a disclosure, particularly where a whistleblower is involved. Carefully delineated channels must be in place to enable staff receiving disclosures (whether through a dedicated hotline or other less formal channels) to escalate them quickly and to the appropriate people. In particular, policies and procedures should name a designated member of the senior management (typically in its legal or compliance function) who should have a direct reporting line to the board or audit committee. Provision should also be made for how to deal with disclosures naming members of the board or the designated senior manager responsible for handling whistleblowing reports.

Even, dispassionate investigation 3.8.1.2

Not every disclosure or whistleblowing report will justify the expenditure of time and resources on comprehensive internal investigations or involve reports to authorities. It is clearly important to guard against complacency or undue cynicism when evaluating issues, or reports by whistleblowers. Level-headedness and even-handedness pay dividends. Allegations should be viewed dispassionately and, where possible, empirically tested by reference to readily available documents, or by means of interviews with relevant individuals (who should be apprised of the importance of confidentiality).

Clear protocol and structure 3.8.1.3

Where initial enquiries show disclosures or allegations to be well founded, firms' responses should be guided by clear protocols setting out the circumstances in which external legal counsel should be instructed (advisable at an early stage to preserve any applicable privilege), how and when other external specialist resources (such as forensic IT consultants or accountants) may be required and instructed, and how such selection and instruction should occur (ideally by legal counsel, again to maintain privilege as far as possible).

Appropriate senior individuals within the firm's human resources function should be involved in coordinating the approach to the whistleblower (if there is one) and dealing with any disciplinary action. The United Kingdom's whistleblowing legislation and the related FCA and PRA whistleblowing rules required some regulated firms to enhance their existing whistleblowing procedures, including by appointing a whistleblowers' champion.

Senior management involvement 3.8.1.4

Once the firm's senior management is notified of serious issues or allegations being made in a whistleblowing report, it is paramount to keep them apprised of the progress of enquiries. If evidence emerges that appears to substantiate the

© Law Business Research 2021

concerns, the window for firms to receive maximum credit for self-reporting to appropriate authorities is relatively short.

3.8.2 Once the decision has been made

Once firms decide to make a report to authorities, the main challenges facing them are to demonstrate that any self-report (1) has been made in a timely fashion, (2) has been made genuinely voluntarily (i.e., not simply because public disclosure or a regulatory or criminal investigation is imminent) and (3) contains enough information to enable the authority to make a meaningful and informed assessment as to how to proceed.

A firm should aim to be the first to self-report to maximise credit. Generally, authorities will acknowledge that internal investigations into complex matters occurring many years before can take time and give credit for initial notifications based on the discovery of certain key facts, with an indication that a fuller report will follow more thorough investigation.

3.8.2.1 Documenting the decision

Regardless of whether the decision is to report or not, it is important for the firm's board to ensure that the issue or allegation is investigated, properly considered with appropriate advice and properly documented. The board must also ensure that appropriate remediation steps are taken, not only to mitigate the risks of criminal, regulatory and civil action, but also to demonstrate the firm's cultural responsiveness and change.

Caution is required in documenting the steps taken in reaching their decisions, not only to preserve privilege as far as possible, but also with regard to the likelihood of such documentation subsequently becoming subjected to external scrutiny or publicity, which is particularly likely for public companies.

3.8.2.2 Nature of approach to the authorities

Self-reports to authorities are not generally made in a set format, but instead usually take the form of a preliminary notification (typically verbal) soon after receiving notice of potential wrongdoing with a more detailed written or oral report after further investigation. The nature and scope of disclosures to authorities vary significantly between, and often within, jurisdictions and may depend on whether the issues cross borders. Specifically, whether it is possible to preserve any applicable privileges by providing reports orally rather than in writing will depend on the circumstances.

3.8.2.3 Timing of a self-report

The SFO requires self-reporting to be made 'within a reasonable time' after the firm becoming aware of the issue, and certainly before the SFO becomes aware of it by some other means, or the firm is threatened with investigation or action by other bodies or authorities, or with leaks or exposure in the press.

© Law Business Research 2021

Beyond potentially impacting the prospects of a DPA, the timing of a self-report will also have a bearing on the decision to prosecute and the level of any potential penalties.

When DPAs were first introduced, the SFO suggested that negotiated settlements would be unlikely where firms had not notified it immediately upon learning of alleged wrongdoing. However, it is increasingly evident that the SFO's expectations as regards timing have become more realistic over time. In speeches to date, Lisa Osofsky has indicated that the SFO will be open to firms investigating allegations of misconduct before reporting.[116]

Managing other regulators 3.8.3

Whatever format they use to report matters to authorities, firms and their advisers should assume that information provided to one enforcement authority will be passed to others, and that referrals may be made where authorities have parallel jurisdiction over some or all aspects of the firm's activities. In cases where the SFO does not prosecute a self-reporting firm, the SFO reserves the right to prosecute for any unreported violations of the law, and may provide information on the reported violation to other bodies (such as foreign police forces or authorities) through the relevant gateway.

The above notwithstanding, firms should not assume that disclosure to one authority necessarily means that other relevant authorities are aware of the matter – full assessments must be made as to whether it is necessary or appropriate to make separate notifications to other specific authorities (whether in the same jurisdiction or elsewhere) who might expect to be told of the alleged misconduct or of the fact of other investigations by or at the behest of enforcement authorities.

116 Lisa Osofsky, SFO Director, speech at the American Bar Association's London White Collar Crime conference alongside Sandra Moser (acting chief of the US Department of Justice's Fraud Section), 8 October 2018.

© Law Business Research 2021

4

Self-Reporting to the Authorities and Other Disclosure Obligations: The US Perspective

Amanda Raad, Sean Seelinger, Jaime Orloff Feeney and Zaneta Wykowska[1]

4.1 Introduction

There is typically no formal obligation in the United States to disclose potential wrongdoing to enforcement authorities; however, there can often be strategic advantages to doing so. Subjects of investigations may, in certain cases, avoid some of the most adverse consequences by self-reporting, including reduced penalties and more favourable settlement terms. Additionally, companies in certain regulated sectors may avoid debarment even where clear violations occurred. US regulators are incentivising companies to self-report by offering potential and meaningful co-operation credit for doing so. The Corporate Enforcement Policy of the US Department of Justice (DOJ), first announced in November 2017, updated and formalised the DOJ's criteria for evaluating and rewarding self-disclosure and co-operation in cases relating to the Foreign Corrupt Practices Act (FCPA). Revisions in March and November 2019 broadened its application beyond the FCPA and clarified the DOJ's expectations for securing credit. More recently, the Corporate Enforcement Policy has been incorporated into the second edition of 'A Resource Guide to the US Foreign Corrupt Practices Act', released by the DOJ and the US Securities and Exchange Commission (SEC) in July 2020.[2]

The Biden administration is expected to continue pursuing FCPA enforcement settlements, consistent with a recently issued Memorandum on

1 Amanda Raad and Sean Seelinger are partners, Jaime Orloff Feeney is counsel and Zaneta Wykowska is an associate at Ropes & Gray LLP.

2 US Dep't of Justice (DOJ) and US Sec. & Exch. Comm'n (SEC), 'A Resource Guide to the U.S. Foreign Corrupt Practices Act' (2d ed. 2020), https://www.justice.gov/criminal-fraud/file/1292051/download.

© Law Business Research 2021

Combating Corruption, which calls for an interagency review to develop a strategy to combat corruption and strengthen enforcement mechanisms.[3] In the first corporate FCPA resolution under the Biden administration, UK-based Amec Foster Wheeler Energy Limited resolved charges that it bribed Brazilian officials in exchange for contracts with the state-owned energy company, Petrobras, including through acts by employees located in New York and Texas.[4]

Although the number of FCPA enforcement cases was down in the beginning of 2020 owing to the covid-19 pandemic, the year closed out with 32 combined FCPA enforcement actions and US$2.78 billion in corporate fines and penalties, compared with 54 FCPA enforcement actions and a combined US$2.6 billion in monetary sanctions in 2019. In November 2020, the DOJ and SEC entered into the largest corporate FCPA resolution to date with Goldman Sachs, which agreed to pay US$2.9 billion in fines as part of a coordinated resolution with authorities in the United States, the United Kingdom, Singapore and elsewhere. In December 2020, the US Commodity Futures Trading Commission (CFTC) also entered into its first foreign corruption-related resolution with Vitol, Inc while Vitol also entered into a parallel resolution with the DOJ.[5] Moreover, US regulators have historically been receptive to parties reporting facts while preserving privilege during the co-operation and reporting process, and are specifically prohibited from making co-operation credit conditional on privilege waiver.

Mandatory self-reporting to authorities 4.2

Before considering a voluntary disclosure, it is important for at least two reasons to determine whether the company has any potential mandatory reporting obligation. First, mandatory reporting obligations often prescribe the recipient, form, timing and content of the disclosure. Second, the evaluation will be materially different if a mandatory report is required, even if that report is in another jurisdiction, given the clear commitment to sharing information between international regulators. In other words, if a company is required to self-report in at least one jurisdiction, it should consider voluntarily disclosing in others given the likelihood that the government agencies will share information.

See Chapter 24 on negotiating global settlements

3 Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest (3 June 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/.

4 See 'Amec Foster Wheeler Energy Limited Agrees to Pay Over $18 Million to Resolve Charges Related to Bribery Scheme in Brazil,' available at https://www.justice.gov/opa/pr/amec-foster-wheeler-energy-limited-agrees-pay-over-18-million-resolve-charges-related-bribery.

5 See 'CFTC Orders Vitol Inc. to Pay $95.7 Million for Corruption-Based Fraud and Attempted Manipulation: First CFTC Enforcement Action Involving Foreign Corruption,' available at https://www.cftc.gov/PressRoom/PressReleases/8326-20.

© Law Business Research 2021

Despite this, the DOJ has adopted a formal policy to avoid 'piling on' penalties that are duplicative for the same misconduct. Under the policy, various US enforcement agencies must coordinate with each other and with foreign government agencies when reaching settlements with corporations. The 2020 FCPA Resource Guide underscores this anti-piling on policy as part of the growing international effort to combat corruption. It includes, as an example, a declination awarded to a UK seismic event detection equipment company, which was subject to a parallel investigation by the Serious Fraud Office (SFO) for the same conduct and committed to accepting responsibility with the SFO.[6] However, the DOJ has warned that companies looking to benefit from the policy should self-disclose wrongdoing directly to the DOJ.[7]

4.2.1 Statutory and regulatory mandatory disclosure obligations

In the United States, most disclosure obligations originate in statute or regulations. Key examples include:

- the Sarbanes-Oxley Act of 2002, which requires the disclosure of all information that has a material financial effect on a public company in periodic financial reports;
- the US Bank Secrecy Act of 1970, which requires financial institutions to disclose certain suspicious transactions or currency transactions in excess of US$10,000;
- the US Anti-Money Laundering Regulations, which require financial institutions to report actual or suspected money laundering under certain circumstances;[8]
- the Anti-Kickback Enforcement Act of 1986, which requires government contractors to make a 'timely notification' of violations of federal criminal law or overpayments in connection with the award or performance of most federal government contracts or subcontracts, including those performed outside the United States; and
- state data breach regulations – all 50 US states have laws requiring companies conducting business in the state to disclose data breaches involving personal information.[9]

6 2020 FCPA Resource Guide, 52–53.

7 When announcing the policy, former Deputy Attorney General Rod Rosenstein specifically remarked that '[c]ooperating with a different agency or a foreign government is not a substitute for cooperating with the Department of Justice'. Rod J Rosenstein, Deputy Att'y Gen., Dep't of Justice, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

8 See, e.g., 31 U.S.C. 5318(g).

9 See Security Breach Notification Laws, National Conference of State Legislatures, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (14 April 2021).

© Law Business Research 2021

Disclosure obligations under agreements with the government 4.2.2

In addition to statutory or regulatory-based mandatory disclosure requirements, companies must also evaluate whether they have any mandatory disclosure obligations under pre-existing agreements with the government. For example, if a company is subject to a deferred prosecution agreement (DPA) (or a corporate integrity agreement (CIA) in the healthcare sector), the agreement often contains self-reporting mandates for any subsequent violations. In many cases, these agreements may require the appointment of independent monitors. While DPAs, CIAs and similar agreements have been used frequently in the United States, other countries, including the United Kingdom, are also now increasingly using similar agreements to drive self-reporting and co-operation.

See Chapter 33 on monitorships

Other sources of mandatory disclosure obligations 4.2.3

Individuals and companies may also have mandatory disclosure obligations as a result of private contractual agreements as well as membership in professional bodies. Such disclosures between private parties may lead to a disclosure to a regulator by the receiving entity. For example, a subcontractor may be obliged by contract to report issues to the contracting party. That contracting party may subsequently determine that it is subject to its own reporting obligation or may choose to self-report to reduce any potential liability.

Voluntary self-reporting to authorities 4.3

Self-reporting and co-operation are important factors for both the DOJ and the SEC in deciding how to proceed with, and resolve investigations and enforcement actions in, cases involving corporations. Companies must carry out a fact-intensive and holistic inquiry in deciding whether to voluntarily self-report to US authorities. There is no one-size-fits-all approach to this analysis, but those contemplating voluntarily disclosing misconduct to US authorities should keep certain considerations in mind.

© Law Business Research 2021

Key Considerations in Resolving Enforcement Actions	
US Department of Justice[10]	**US Securities and Exchange Commission**[11]
• Self-disclosure and willingness to co-operate in the investigation • Disclosure of individuals substantially involved in or responsible for misconduct • Pervasiveness of wrongdoing within the corporation • Existence and effectiveness of a compliance programme • Meaningful remedial actions	• Self-reporting and investigation of misconduct • Effective compliance procedures and appropriate tone at the top • Whether the case involves a potentially widespread industry practice • Whether the conduct is ongoing • Remediation, including dismissing or disciplining wrongdoers

4.3.1 Advantages of voluntarily self-reporting

The primary benefit to self-reporting is to secure potentially reduced penalties through co-operation credit and, moreover, to maintain control over the flow of information to regulators. In recent years, US regulators have become increasingly vocal about the benefits of self-disclosure and co-operation, with the DOJ even formalising those benefits, first, in its FCPA Pilot Program (Pilot Program)[12] and subsequently the Corporate Enforcement Policy. Yet, co-operation, which inevitably goes hand in hand with a voluntary disclosure, imposes significant demands on corporations and is not without meaningful risk.

4.3.1.1 DOJ co-operation credit

To encourage self-reporting and co-operation, the DOJ has issued and subsequently revised guidance on the subject for many years. In June 1999, the then Deputy Attorney General Eric Holder issued the Principles of Federal Prosecution of Business Organizations, now known as the 'Holder Memorandum', to articulate and standardise the factors to be considered by federal prosecutors in making charging decisions against corporations.[13] The Holder Memorandum instructed DOJ prosecutors to consider as a factor in bringing charges whether a corporation has timely and voluntarily disclosed wrongdoing and whether it has been willing 'to cooperate in the investigation

10 See FCPA Corporate Enforcement Policy, DOJ, Justice Manual, § 9-47.120, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120 (Corporate Enforcement Policy).

11 See Enforcement Manual, SEC Division of Enforcement (28 November 2017), available at https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

12 For more details, see 'The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance', available at https://www.justice.gov/opa/file/838386/download (FCPA Enforcement Plan and Guidance).

13 Memorandum from Eric Holder, Deputy Att'y Gen., Dep't of Justice, on Bringing Criminal Charges Against Corps. to Dep't Component Heads and U.S. Attorneys (16 June 1999), available at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF.

© Law Business Research 2021

of its agents'.[14] In 2008, then-Deputy Attorney General Mark R Filip added language to the US Attorneys' Manual, now titled the Justice Manual,[15] instructing prosecutors to consider 'the corporation's willingness to provide relevant information and evidence and identify relevant actors within and outside the corporation, including senior executives' when assessing a corporation's co-operation.[16] Mr Filip also outlined in his memorandum nine factors on which prosecutors should base their corporate charging and resolution decisions, the so-called 'Filip Factors', incorporating some language from the Holder Memorandum (Filip Factor Four, a corporation's 'willingness to cooperate in the investigation of [its] agents'), and adding Filip Factor Eight: 'the adequacy of prosecution of individuals responsible for the corporation's malfeasance'.

The Yates Memorandum

Building on the Holder Memorandum, then-Deputy Attorney General Sally Quillian Yates issued the Memorandum of Individual Accountability for Corporate Wrongdoing, now known as the 'Yates Memorandum', in September 2015. The Yates Memorandum outlines the 'six key steps' prosecutors should take in all investigations of corporate wrongdoing. The most significant policy shift in the Yates Memorandum concerned the relationship between a company's co-operation with respect to individual wrongdoers and the company's eligibility for co-operation credit. Under the Yates Memorandum, the identification of responsible individuals became a 'threshold requirement' for receiving any co-operation credit consideration. Ms Yates also emphasised that a failure to conduct a robust internal investigation is not an excuse, stating that '[c]ompanies may not pick and choose what facts to disclose'.

Former Deputy Attorney General Rod Rosenstein announced a shift in the DOJ's policy in 2018. Under the revised policy, a corporation was entitled to co-operation credit in criminal proceedings as long as it disclosed 'all relevant facts known to it *at the time of the disclosure*, including as to any individuals *substantially* involved in or responsible for the misconduct at issue'.[17] On 28 October 2021, however, Deputy Attorney General Lisa Monaco announced that the DOJ is reinstating the requirements outlined in the Yates Memorandum. Monaco stated that in order to receive co-operation credit, 'companies must provide the department with all non-privileged information

14 Id. at 3 (listing eight factors prosecutors should consider in deciding whether to bring charges against corporations that include '[t]he corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents').

15 US Dep't of Justice, Justice Manual §§ 9-28.000.

16 Id. §§ 9-28.700 – Value of Cooperation.

17 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0 (emphasis added).

© Law Business Research 2021

about individuals involved in or responsible for the misconduct at issue', regardless of position, status or seniority.[18]

However, the Justice Manual, which was revised in 2018, continues to specify that '[t]here may be circumstances where, despite its best efforts to conduct a thorough investigation, a company genuinely cannot get access to certain evidence or is actually prohibited from disclosing it to the government'.[19] Nevertheless, the Justice Manual is clear that in such cases 'the company seeking cooperation will bear the burden of explaining the restrictions it is facing to the prosecutor'.[20] Consequently, thorough and properly scoped internal investigations are of critical importance.

The Corporate Enforcement Policy

In November 2017, the DOJ announced that it would be incorporating its Corporate Enforcement Policy to incentivise voluntary self-disclosure of misconduct into the Justice Manual, following on from a successful Pilot Program in 2016.[21] On 1 March 2018, the DOJ announced that it would apply the Corporate Enforcement Policy as non-binding guidance in criminal cases outside the FCPA context.[22] Moreover, the most substantial addition to the 2020 FCPA Resource Guide is a section incorporating the Corporate Enforcement Policy, underscoring the DOJ's and SEC's emphasis on voluntary self-disclosure, co-operation and remediation. In light of these developments, the Corporate Enforcement Policy provides valuable guidance to corporations as they investigate misconduct and contemplate voluntary disclosure.

The Corporate Enforcement Policy outlines the requirements for a company to earn credit for voluntary self-disclosure. The disclosure must (1) occur prior to an imminent threat of disclosure or government investigation, (2) be disclosed within a reasonably prompt time after the company becomes aware of the offence and (3) include all relevant facts known to the company at the time of disclosure, including all relevant facts about the individuals substantially involved in or responsible for the misconduct.[23] The November 2019 changes to the Corporate Enforcement Policy acknowledge the DOJ's recognition, in a footnote, that 'a company may not be in a position to know all relevant facts at the time of a voluntary self-disclosure'. The Corporate Enforcement Policy also now requires the company to alert the DOJ of evidence of the misconduct

18 Lisa O Monaco, Deputy Atty Gen., DOJ, Keynote Address at ABA's 36th National Institute on White Collar Crime (28 October 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

19 Justice Manual § 9-28.700.

20 Id.

21 See Corporate Enforcement Policy.

22 See Jody Godoy, 'DOJ Expands Leniency Beyond FCPA, Lets Barclays Off', *Law360*, 1 March 2018, https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off.

23 Corporate Enforcement Policy.

© Law Business Research 2021

when it becomes aware of it, whereas, previously, where the company was or should have been aware of opportunities for the DOJ to obtain evidence not in the company's possession, it had to identify those opportunities to the DOJ to receive full co-operation credit.

In addition, the Corporate Enforcement Policy contains specific guidance on the steps a company must take to earn full co-operation credit and to provide timely and appropriate remediation, consistent with the Yates Memorandum and the Justice Manual's Sentencing Guidelines. The exact level of co-operation credit available to a corporation will vary based on the investigation. It is possible for a corporation to earn full credit under the US Sentencing Guidelines but not earn additional credit under the Corporate Enforcement Policy.[24] Moreover, the DOJ has shown itself willing to assign different levels of co-operation credit for different investigations into the same company. For example, in June 2019, the DOJ entered a non-prosecution agreement (NPA) with Walmart, resolving investigations into Walmart's alleged corrupt activity in four countries: Brazil, China, India and Mexico. Although the NPA covered conduct in all four countries, and the company received full credit for its co-operation with the DOJ in the first three investigations, with respect to the Mexico investigation, Walmart received only partial credit due to its failure to timely provide certain documents and 'deconflict' in response to a witness interview request.

See Chapter 10 on co-operating with authorities

The Corporate Enforcement Policy provides benefits to a company that satisfies all the requirements for voluntary self-disclosure, co-operation and remediation. Companies that fully co-operate with DOJ investigations and implement appropriate remediation in FCPA matters, but that do not voluntarily self-disclose, will be eligible for limited credit, at most a 25 per cent reduction off the bottom of the Sentencing Guidelines fine range. However, when a company has voluntarily self-disclosed, fully co-operated with the DOJ, and has timely and appropriately remediated, the Corporate Enforcement Policy creates a rebuttable presumption, which may be overcome by 'aggravated circumstances' related to the nature and seriousness of the offence, that the DOJ will grant a declination.[25] Under the Corporate Enforcement Policy, if the presumption is overcome and a criminal resolution is warranted, the DOJ will recommend a 50 per cent reduction off the low end of the Sentencing Guidelines fine range and generally will not require the appointment of a

24 The DOJ evaluated corporate co-operation in this manner when reaching its DPA with Mobile TeleSystems in February 2019. See https://www.justice.gov/opa/press-release/file/1141631/download.

25 Corporate Enforcement Policy at § 1. 'Aggravating circumstances that may warrant a criminal resolution include, but are not limited to, involvement by executive management of the company in the misconduct; a significant profit to the company from the misconduct; pervasiveness of the misconduct within the company; and criminal recidivism.'

© Law Business Research 2021

See Chapter 46 on compliance

monitor if the company has, at the time of resolution, implemented an effective compliance programme.[26]

The DOJ has issued 14 public declinations under the Corporate Enforcement Policy and the earlier Pilot Program.[27] The DOJ last issued a declination in August 2020, when the DOJ declined to prosecute World Acceptance Corporation due to its voluntary self-disclosure, extensive co-operation and remediation, and disgorgement of US$17.8 million.[28]

By publishing its rationale for issuing declinations, the DOJ has sought to provide 'increased transparency as to [the] evaluation process'.[29] However, in a June 2019 speech to the American Bar Association, former Deputy Assistant Attorney General Matt Miner announced that the DOJ would be open to keeping declinations private where public release is 'neither necessary nor warranted'. Miner gave the example of a corporation that discovers inconsequential bribes in an M&A transaction and self-discloses immediately – in such a case, the agency would be 'open to discussion' regarding public release. Nonetheless, Miner maintained that this decision will always remain in the agency's discretion.

The following table outlines several recent FCPA corporate resolutions under the Corporate Enforcement Policy, and the comparative credit for self-disclosure, co-operation and remediation.

26 Corporate Enforcement Policy at § 1. The Enforcement Policy provides specific guidance on the criteria for evaluating a corporate compliance programme, while also noting that the criteria may vary based on the size and resources of an organisation. Factors listed in the policy include culture of compliance, compliance resources, the quality and experience of compliance resources, independence and authority of the compliance function, effective risk assessments and risk-based approach, compensation and promotion of compliance employees, compliance-related auditing, and compliance reporting structure.

27 See https://www.justice.gov/criminal-fraud/corporate-enforcement-policy/declinations.

28 See https://www.justice.gov/criminal-fraud/file/1301826/download.

29 Matt Miner, Deputy Assistant Att'y Gen., Dep't of Justice, Remarks at The American Bar Association, Criminal Justice Section Third Global White Collar Crime Institute Conference (27 June 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matt-miner-delivers-remarks-american-bar-association.

© Law Business Research 2021

Recent Resolutions under DOJ's Corporate Enforcement Policy	
Amec Foster Wheeler Energy Limited (AFWEL)	
Background	AFWEL, a subsidiary of UK-based Wood Group, is a British multinational consultancy, engineering and project management company. Between 2011 and 2014, AFWEL bribed Brazilian officials in return for a US$190 million contract to design a gas-to-chemicals facility. AFWEL admitted conspiring with a Monaco-based intermediary, an Italian sales agent and a store manager in New York City to pay bribes to Petrobas officials to secure the project. AFWEL's compliance process identified red flags in the transaction, but the agent was allowed to continue the transactions unofficially
Self-Report	AFWEL did not voluntarily self-report
Co-operation and Remediation	AFWEL received full credit for its cooperation with the investigation as it made factual presentations, voluntarily facilitated the interview in the United States of former foreign-based employees and produced extensive documentation
Result	In June 2021, AFWEL entered into a DPA with the DOJ and a related resolution with the SEC. AFWEL agreed to pay a criminal penalty of US$18.375 million. The criminal penalty was reduced by 25 per cent from the applicable US Sentencing Guidelines range as AFWEL committed to full co-operation and remediation, which involved terminating an individual involved in the misconduct and adopting heightened controls and anti-corruption procedures
World Acceptance Corporation (WAC)	
Background	WAC's Mexican subsidiary paid approximately US$4.1 million in bribes between 2010 and 2017 to obtain and retain business relating to its Préstamos Viva business line, which offered small loans to state and federal government employees
Self-Report	WAC voluntarily self-disclosed to the DOJ on learning of the misconduct
Co-operation and Remediation	WAC proactively co-operated with the DOJ, including provision of known relevant facts about the misconduct, and took steps to remediate, including by providing additional FCPA training as part of its compliance programme. WAC also separated from executives under whom the misconduct took place and discontinued its relationships with third parties involved in the misconduct
Result	In August 2020, the DOJ issued a declination letter, while the SEC issued a cease and desist order requiring WAC to disgorge US$17.8 million, prejudgment interest of US$1.9 million and a US$2 million civil fine
Quad/Graphics Inc (Quad/Graphics)	
Background	Quad/Graphics is a US-based digital and print marketing provider. Between 2011 and 2016, employees of Quad/Graphics' Peruvian subsidiary paid or promised to pay over US$1 million to intermediaries, in part, to pay bribes to Peruvian officials to secure printing contracts and minimise penalty and tax payments. Additionally, between 2010 and 2015, employees of Quad/Graphics' Chinese subsidiary paid bribes to employees of state-owned companies to secure printing business in China
Self-Report	Quad/Graphics voluntarily and promptly self-disclosed to the DOJ
Co-operation and Remediation	Quad/Graphics conducted an internal investigation, proactively co-operated with the DOJ, took steps to enhance its compliance programme and terminated relationships with employees and third parties involved in the misconduct
Result	In September 2019, the DOJ issued a declination letter and the SEC issued a cease and desist order requiring Quad/Graphics to disgorge US$6.9 million in profits, plus interest and pay a US$2 million civil penalty

© Law Business Research 2021

Recent Resolutions under DOJ's Corporate Enforcement Policy	
Telefonaktiebolaget LM Ericsson (Ericsson)	
Background	Ericsson is a multinational telecommunications company headquartered in Sweden. Ericsson admitted that between 2000 and 2016, it used third parties to make bribe payments to government officials or to manage off-the-books slush funds in Djibouti, China, Vietnam, Indonesia and Kuwait
Self-Report	Ericsson did not voluntarily self-report
Co-operation and Remediation	Ericsson did not receive full credit for co-operation and remediation because it did not disclose allegations of corruption with respect to two relevant matters, produced certain materials in an untimely manner and did not fully remediate, including by failing to take adequate disciplinary measures with respect to certain employees involved in the misconduct
Result	In December 2019, Ericsson entered into a DPA with the DOJ and a related resolution with the SEC. Ericsson agreed to pay a criminal penalty of US$520.7 million and US$539.9 million in disgorgement of profits under its civil resolution with the SEC. The criminal penalty was reduced by 15 per cent off the applicable US Sentencing Guidelines range because Ericsson committed to further enhance its compliance programme and internal accounting controls. Ericsson's Egyptian subsidiary pleaded guilty to conspiracy to violate the anti-bribery provisions of the FCPA. Ericsson also agreed to the imposition of an independent compliance monitor

The Corporate Enforcement Policy and the Pilot Program before it have demonstrated the DOJ's commitment to rewarding voluntary self-disclosure in FCPA enforcement, and by many accounts has been viewed as very successful.

Benczkowski Memorandum

As part of the DOJ's ongoing effort to update and clarify its corporate enforcement policies, in October 2018, the then Assistant Attorney General Brian Benczkowski issued new guidance on imposing corporate compliance monitors, which is now known as the 'Benczkowski Memorandum'.[30] The policy supplemented the 2008 'Morford Memorandum', which outlined the principles on selection, scope and duration of monitorships, and supersedes the guidance contained in the 2009 'Breuer Memorandum' on imposing corporate monitors. Former Assistant Attorney General Brian Benczkowski explained that the goal of the new guidance was to 'further refine the factors that go into the determination of whether a monitor is needed, as well as clarify and refine the monitor selection process'.

Under the Benczkowski Memorandum, the potential benefits of employing a corporate monitor should be weighed against the cost of a monitor and

30 Memorandum from Brian A. Benczkowski, Assistant Att'y Gen., Dep't of Justice, (11 October 2018), Selection of Monitors in Criminal Division Matters, available at https://www.justice.gov/opa/speech/file/1100531/download (Benczkowski Memorandum); 'Assistant Attorney General Brian A. Benczkowski Delivers Remarks at NYU School of Law Program on Corporate Compliance and Enforcement Conference on Achieving Effective Compliance', available at https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-nyu-school-law-program.

© Law Business Research 2021

its impact on the operations of the corporation. In making a determination to impose a corporate monitor, the DOJ will consider a number of factors, including the type of misconduct, the pervasiveness of the conduct and whether it involved senior management, the investments and improvements a company has made to its corporate compliance programme and internal controls, and whether those improvements have been tested to demonstrate that they would prevent or detect similar misconduct in the future. Other factors include whether remedial actions were taken against individuals involved, and the industry and geography in which the company operates and the nature of the company's clientele. The Benczkowski Memorandum provides: 'Where a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not be necessary.'[31]

A key feature of the Benczkowski Memorandum is that companies can receive meaningful credit, namely avoiding a compliance monitor, by engaging in extensive remediation of their compliance programmes. The DOJ did not impose a monitor in connection with any enforcement actions in 2020, compared to three in 2019. However, Deputy Attorney General Monaco's remarks on 28 October 2021 signalled that the DOJ may make more use of monitors going forward. Monaco made clear that the DOJ 'is free to require the imposition of independent monitors whenever it is appropriate to do so in order to satisfy our prosecutors that a company is living up to its compliance and disclosure obligations' and to the extent that prior guidance suggested 'that monitorships are disfavored or are the exception', that guidance is rescinded.[32]

See Chapter 33 on monitorships

SEC co-operation credit 4.3.1.2

Although it can be difficult to precisely quantify the benefit of co-operation with the SEC, the Commission will consider general principles of sentencing, especially general deterrence. In both public statements and in practice, the Commission has made clear that companies can receive significant leniency for full co-operation. During a speech on 9 May 2018, former SEC Enforcement Division Co-Director Steven Peikin emphasised the importance of co-operation, noting that the SEC would continue to provide 'incentives to those who come forward and provide valuable information' to the SEC.[33] Co-operation may influence the Commission's decision whether to impose a civil monetary penalty.[34]

31 Benczkowski Memorandum at 2.

32 Lisa O Monaco, Deputy Atty Gen., DOJ, Keynote Address at ABA's 36th National Institute on White Collar Crime (see supra note 18)

33 See 'Keynote Address at the New York City Bar Association's 7th Annual White Collar Crime Institute', available at https://www.sec.gov/news/speech/speech-peikin-050918.

34 In its November 2018 resolution with Vantage Drilling International, the SEC cited co-operation and financial condition as its basis for not imposing a fine. See https://www.sec.gov/litigation/admin/2018/34-84617.pdf.

© Law Business Research 2021

While the SEC has not entered into any NPAs since 2016 and has only entered into three since their inception in 2010,[35] the SEC nevertheless signalled its continued commitment to using NPAs to reward co-operation through amendments, passed in September 2020 to the rules governing monetary awards to whistleblowers. Specifically, the amendments clarify the SEC's ability to make award payments to whistleblowers based on money collected as a result of DPAs and NPAs entered into by the DOJ and SEC, to 'ensure that whistleblowers are not disadvantaged because of the particular form of an action' that the applicable authority takes.[36] The SEC will, however, set a high bar before entering into an NPA in an FCPA enforcement action. With respect to NPAs entered into with Akamai Technologies, Inc and Nortek, Inc in 2016, Kara Brockmeyer, then-Chief of the SEC Enforcement Division's FCPA Unit, stated: 'Akamai and Nortek each promptly tightened their internal controls after discovering the bribes and took swift remedial measures to eliminate the problems. They handled it the right way and got expeditious resolutions as a result.'[37]

4.4 Risks in voluntarily self-reporting

While self-disclosure can reap significant monetary benefits, a company must balance the potential risks against any potential benefit. Self-reporting can give rise to lengthy co-operation obligations and increased government scrutiny. As discussed above, the multi-jurisdictional nature of many 'white-collar' matters means that self-reporting may lead to enquiries from global regulators, differing resolutions and ongoing obligations.

Furthermore, the DOJ is likely to impose a stringent bar when evaluating the sufficiency of compliance programmes to determine whether the requirements of the Corporate Enforcement Policy are met or to otherwise reduce liability. On 1 June 2020, the DOJ published revised guidance on Evaluation of Corporate Compliance Programs[38] (the Guidance), first released in February 2017 and updated in April 2019. The Guidance is framed around

See Chapter 46 on compliance

35 The SEC announced its first NPA in an FCPA case in 2013, when it entered into an NPA with Ralph Lauren Corporation relating to bribes paid to government officials in Argentina. See 'SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct', available at https://www.sec.gov/news/press-release/2013-2013-65htm. The SEC announced its second and third NPAs on 7 June 2016. See 'SEC Announces Two Non-Prosecution Agreements in FCPA Cases', available at https://www.sec.gov/news/pressrelease/2016-109.html.

36 See 'SEC Adds Clarity, Efficiency and Transparency to Its Successful Whistleblower Award Program,' available at https://www.sec.gov/news/press-release/2020-219.

37 See 'SEC Announces Two Non-Prosecution Agreements in FCPA Cases', available at https://www.sec.gov/news/pressrelease/2016-109.html.

38 US Dep't of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (updated June 2020), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

© Law Business Research 2021

three fundamental questions as to whether (1) the corporation's compliance programme is well designed, (2) it is being applied earnestly and in good faith (i.e., whether it is adequately resourced and empowered to function effectively), and (3) it works in practice. The Guidance has since also been incorporated into the 2020 FCPA Resource Guide, which notes the DOJ's position that 'the truest measure of an effective compliance program is how it responds to misconduct'.

Although the content of the Guidance is largely familiar to practitioners, it does give a clearer picture of the DOJ's current approach to corporate compliance. The Guidance underscores the DOJ's focus on the operation, rather than the appearance, of corporate compliance programmes. The Guidance suggests that companies should expect to be asked detailed and challenging questions regarding the scope and effectiveness of their compliance programmes, both at the time of the offence and at the time of the charging decision and resolution. The Guidance emphasises the DOJ's expectation that compliance programmes should be risk-based and tailored to the specific commercial realities of the company's business, and that companies should continually reassess their risk profiles and the efficacy of their compliance programmes to ensure their programmes are fit to address evolving risks and trends. Moreover, the Guidance makes clear that the DOJ will enquire about the company's culture of compliance at all levels of the business, including middle management as well as senior management, and whether the company's compliance function has sufficient access to data across the business and makes use of data analytics to monitor and test policies, controls, and transactions. In the mergers and acquisitions context, the Guidance emphasises the need for pre-acquisition compliance due diligence as well as post-closing integration.

If a company's compliance programme fails to withstand such scrutiny, it risks losing credit for the programme, paying higher penalties or even facing separate violations for inadequate internal controls. Taking these existing increasingly stringent co-operation standards into consideration, companies considering self-disclosure should carefully assess whether they can meet regulator expectations. If companies fall short, regulators may refuse co-operation credit and use the information obtained through the self-disclosure against the company.

Risks in choosing not to self-report 4.5

US regulators have warned that the potential downside of not self-reporting any violation could be significant where the matter is otherwise brought to their attention. In an October 2020 press release announcing a DPA and US$19.6 million settlement with Chicago-based Beam Suntory, Inc to resolve an investigation into bribery of Indian officials for approval of a licence to bottle a line of products in India, the DOJ noted that Beam did not timely disclose the conduct that triggered the investigation, took positions that were

© Law Business Research 2021

not consistent with co-operation and caused significant delays in reaching a resolution by refusing to accept responsibility for several years.[39]

Consequently, companies should carefully consider the likelihood that the conduct will be discovered by other means. It is important to consider whether other industry players could affect the company's position. Industry-wide trends may expose a company's misconduct. If regulators undertake an industry-wide investigation into particular practices, which we have observed in recent years with pharmaceutical companies, medical device manufacturers and automobile companies, a company might be exposed by a competitor's self-report or more passively through a third-party subpoena or any investigative demand.

Companies should also be sensitive to increasing whistleblower activity. Current or former employees are incentivised to report potential misconduct to US regulators, which has led to substantial recoveries for the government. The SEC's whistleblower programme has been steadily active, with 233 individuals receiving approximately US$1.2 billion between 2012 and November 2021.[40] Whistleblowers are eligible to receive awards between 10 per cent and 30 per cent of the money recovered if their 'high-quality original information' leads to enforcement actions in which the SEC orders at least US$1 million.[41] Moreover, the SEC's 2020 amendments to the rules governing the whistleblower award programme provide that for awards where the statutory maximum amount is US$5 million or less, there is a presumption that the SEC will pay the claimaint the 30 per cent maximum statutory award unless there are negative award criteria present, subject to certain limitations.[42] The programme continues to be a priority for the Commission. In October 2020, the SEC announced its largest whistleblower award to date, with a single whistleblower receiving over US$114 million.[43] It is therefore important that a company consider the real possibility that its conduct could be exposed by means other than voluntary self-disclosure, and the associated, often expensive, risks associated with not being the first to come forward. When deciding not to self-report, a company must ensure that the decision is appropriately considered and documented. If a company decides not to self-report and the government later enquires about the issue, the best defence is that the company conducted a thorough investigation, remediated the issue and had a reasonable

39 See 'Beam Suntory Inc. Agrees to Pay Over $19 Million to Resolve Criminal Foreign Bribery Case', available at https://www.justice.gov/opa/pr/beam-suntory-inc-agrees-pay-over-19-million-resolve-criminal-foreign-bribery-case.

40 See 'SEC Issues Whistleblower Awards Totaling Approximately $10.4 Million,' available at https://www.sec.gov/news/pressrelease/2021-243.

41 More information is available at the SEC's 'Office of the Whistleblower' site at https://www.sec.gov/whistleblower.

42 See 'SEC Adds Clarity, Efficiency and Transparency to Its Successful Whistleblower Award Program', available at https://www.sec.gov/news/press-release/2020-219.

43 See 'SEC Issues Record $114 Million Whistleblower Award', available at https://www.sec.gov/news/press-release/2020-266.

© Law Business Research 2021

basis for not self-reporting to the government. US regulators will look to a company's board of directors to ensure the appropriate steps were taken.[44] The SEC has expressed that the board of directors must exercise oversight and set a strong 'tone at the top' emphasising the importance of compliance.

44 Notification of the board of directors is often required under federal securities law. s.307 Sarbanes-Oxley Act of 2002 requires that an attorney report evidence of a material violation of securities laws or breach of fiduciary duty by the company or any agent 'up-the-ladder' (i.e., first to the chief legal officer or CEO and, thereafter, if appropriate remedial measures are not taken, to the audit committee of the board or other board committee comprised solely of non-employee directors). Wherever possible, it is best to engage the board's disclosure counsel to assist in making this determination.

© Law Business Research 2021

5

Beginning an Internal Investigation: The UK Perspective

Jonathan Cotton, Holly Ware and Ella Williams[1]

5.1 Introduction

Company investigations arise from a diverse range of sources: from internal issues such as employee allegations, whistleblowing, supplier or customer complaints and audit findings, to external triggers such as reports in the press, on blogs and on social media, allegations in third-party litigation and approaches from regulators or other authorities, who may independently have uncovered an issue.

The focus of this chapter is on the factors relevant to a company's decision whether, when and how to launch an internal investigation, and to highlight key considerations in conducting the early stages of an internal investigation. These decisions are often made under significant time pressure, and with only limited information, but they can have serious repercussions.

5.2 Whether to notify any relevant authorities

See Chapter 3 on self-reporting

A key initial question when a potential issue comes to light is whether to notify any relevant authorities – which is likely, in turn, to impact several aspects of the internal investigation. Whether a notification is required or desirable will turn on the regulatory status of the company or the individuals uncovering the issue, the expectations of the relevant authorities and the issue itself.

Firms regulated by the Financial Conduct Authority (FCA) are under a duty to deal with their regulators openly and co-operatively and to disclose appropriately anything relating to them of which the FCA would reasonably

1 Jonathan Cotton and Holly Ware are partners and Ella Williams is senior counsel at Slaughter and May. The authors would like to thank Anna Lambourn, a professional support lawyer at the firm, for her assistance in preparing this chapter.

© Law Business Research 2021

expect notice.[2] The FCA Handbook sets out a non-exhaustive list of situations where a firm is under an explicit duty to notify.[3] Although the timing of the notification will depend on the circumstances, the FCA expects a firm to discuss relevant matters with it 'at an early stage, before making any internal or external commitments', and in certain cases the notification obligation can be immediate.[4] Dual-regulated firms owe similar obligations to the Prudential Regulation Authority.[5]

Obligations to notify may also arise under anti-money laundering legislation. Persons working in the 'regulated sector' (a wider concept than just firms regulated by the FCA) must submit (subject to certain limited exceptions) a suspicious activity report (SAR) to the National Crime Agency in respect of information that comes to them in the course of their business if they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, or even just attempting the latter.[6] Even if a person does not work in the 'regulated sector', they may still need to make a SAR and an accompanying application for a 'defence against money laundering' to avoid the risk of committing a money laundering offence if they suspect that property they are dealing with is in some way criminal.[7]

Other notification requirements may arise under the rules of professional bodies[8] or under data privacy legislation.[9]

While there is no general legal obligation to report crime to the authorities, it may be in a company's interests to self-report suspicions of criminal conduct

2 Financial Conduct Authority (FCA) Handbook, PRIN 2.1.1R, Principle 11. Individuals subject to the FCA's individual conduct rules are also subject to equivalent obligations under FCA Handbook, Code of Conduct (COCON) 2.1.3 and COCON 2.2.4.

3 FCA Handbook, SUP 15.3.

4 ibid.

5 Prudential Regulation Authority (PRA) Rulebook, Notifications, Rule 2. (A dual-regulated firm is a firm that is a 'bank, a building society or a UK designated investment firm', FCA Handbook, SYSC 19 D.) The equivalent for PRA-authorised persons within the meaning of s.2B(5) Financial Services and Markets Act 2000 (FSMA) is Fundamental Rule 7 of the PRA Rulebook: A firm must deal with its regulators in an open and cooperative way and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice.

6 Proceeds of Crime Act 2002, ss.330 and 331 and Terrorism Act 2000, s.21A. 'Regulated sector' is defined in the Proceeds of Crime Act 2002, Schedule 9.

7 Proceeds of Crime Act 2002, ss.335 and 338.

8 For example, firms of solicitors have an obligation to report certain matters to the Solicitors Regulation Authority (SRA) (see, for example, Rule 3 (Cooperation and Accountability), Code of Conduct for Firms, SRA Standards and Regulations) and accountants regulated by the Institute of Chartered Accountants in England and Wales are subject to a reporting obligation under Disciplinary Bye-laws 9.1 and 9.2.

9 For example, there could be a requirement to notify the Information Commissioner's Office if a personal data breach may have occurred (see Regulation (EU) 2016/679 (General Data Protection Regulation), Article 33; Data Protection Act 2018, s.67).

© Law Business Research 2021

to the Serious Fraud Office (SFO). The Deferred Prosecution Agreements Code of Practice (the DPA Code) states that it will be a public interest factor against prosecution if a company self-reports 'within a reasonable time of the offending coming to light';[10] a point that has been strongly endorsed by the courts in the DPA judgments handed down to date,[11] and which is reflected in the SFO's 'Corporate Co-operation Guidance' and the 'Deferred Prosecution Agreements' chapter in its Operational Handbook.[12] It has been acknowledged by the Director of the SFO that 'reasonable time' allows a company to conduct at least a preliminary investigation into a potential issue before self-reporting.[13]

See Chapters 3 on self-reporting to authorities and 23 on negotiating global settlements

Finally, certain companies will need to consider whether they are required (both at the outset of the investigation and on an ongoing basis) to make a disclosure to the market in relation to the potential issue that has come to light. If a market disclosure is required then it is easier to conclude that the company should also inform the relevant authorities.[14]

5.3 Whether and when to launch an internal investigation

Conducting an investigation is not without risk, and the risks should be considered carefully before an internal investigation starts. Once begun, an investigation can be difficult to stop or limit without damaging the company's credibility.

There can be a significant number of advantages to undertaking an internal investigation, including, principally, the ability to gain a better understanding of the facts to allow for more informed decision-making and the exploration

10 Deferred Prosecution Agreements Code of Practice, para. 2.8.2(i).

11 See, e.g., *Serious Fraud Office v. Standard Bank Plc (now known as ICBC Standard Bank Plc)* [2016] Lloyd's Rep FC 102, at para. 14; *Serious Fraud Office v. Tesco Stores Ltd* [2019] Lloyd's Rep FC 283, at paras. 66 and 117; *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at para. 47; *Serious Fraud Office v. Airline Services Limited* [2020] 10 WLUK 606, at para. 52; *Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep FC Plus 27, at para. 35.

12 Serious Fraud Office (SFO) Operational Handbook, Corporate Co-operation Guidance, August 2019, p. 1 (co-operation includes 'identifying suspected wrongdoing and criminal conduct . . . reporting this to the SFO within a reasonable time of the suspicions coming to light') and Deferred Prosecution Agreements, October 2020 ('[v]oluntary self-reporting suspected wrongdoing within a reasonable time of those suspicions coming to light is an important aspect of co-operation').

13 In a speech on 3 April 2019, Lisa Osofsky, Director SFO, said that companies 'have a duty to their shareholders to ensure allegations or suspicions are investigated, assessed and verified, so they understand what they may be reporting before they report it': available at https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/.

14 If applicable and the findings constitute inside information under the EU Market Abuse Regulation (transcribed into UK law via the European Union (Withdrawal) Act 2018 (as amended), as supplemented by The Market Abuse (Amendment) (EU Exit) Regulations 2019 (UK MAR)), the issuer would need to make such a disclosure. (UK MAR, Article 17(1): the issuer shall inform the public as soon as possible of inside information which directly concerns the issuer).

© Law Business Research 2021

of possible defences, and to increase a company's ability to react effectively to any external investigations or adverse publicity. There can also be significant financial benefits if the results of the investigation allow the company to apply for leniency or immunity (principally available in the competition sphere) or to self-report and co-operate with an external investigation to gain a discount on a potential future financial penalty (or avoid prosecution altogether). Undertaking an internal investigation can also help to demonstrate that a company has adequate procedures and a corporate culture that takes compliance seriously, with wider benefits should the company's compliance framework later be evaluated. Linked to this, an internal investigation can also allow for proper remediation and the implementation of compliance enhancements that might help to avoid similar issues arising in future.

Sometimes, the factors in favour of conducting an internal investigation are acute. For example, where a company has to investigate to comply with its regulatory obligations (for instance the FCA Principles for Businesses)[15] or for directors to comply with their fiduciary and other statutory or common law duties.[16] A company may also have existing internal corporate governance codes or compliance policies that mandate an investigation. On the other hand, authorities have been known to request that companies do not conduct an internal investigation at all (for instance if it risks employees being 'tipped off' that they are under investigation, denying the authority the chance to monitor the relevant individuals covertly). Indeed, the FCA has stated that: 'Whether and how a firm investigates internally must now be looked at from the point of view of whether doing so will assist or inhibit the FCA's investigation.'[17]

There are, however, a number of potential downsides to conducting an internal investigation, which may in certain circumstances lead a company to decide not to investigate. These downsides include the potentially high costs and resource requirements of an investigation (including distraction from business as usual) and the reputational risk that might occur should the investigation become public. An investigation may, depending on its outcome, mean that companies have to notify stakeholders (such as insurers, auditors, lenders – particularly where the facts may constitute an event of default – and third-party customers), or make a disclosure to the market. There is also the risk that the internal investigation might result in the creation of non-privileged documents that could assist regulators, prosecutors or potential civil claimants (such as customers or shareholders), to the detriment of the company, and the risk that the investigation might uncover misconduct beyond the scope of the initial allegation.

15 FCA Handbook, PRIN 2.1.1R.

16 See, in particular, Companies Act 2006, ss.171 to 177.

17 Speech by Jamie Symington, then Director in Enforcement – Wholesale, Unauthorised Business and Intelligence, FCA (5 November 2015), available at https://www.fca.org.uk/news/speeches/internal-investigations-firms. See also FCA Handbook, Enforcement Guide (EG) 3.11.7.

© Law Business Research 2021

When deciding whether and when to conduct an internal investigation, companies will also consider whether to instruct external legal counsel to advise on or conduct the investigation. In addition to providing investigations expertise and additional personnel, the engagement of external counsel can also bolster the independence of the investigation, which is important in a criminal or regulatory context, and provide an external viewpoint to balance the views of internal stakeholders. Engaging external counsel also increases the likelihood that privilege may apply to investigation documents.

5.4 Oversight and management of the investigation

One of the first issues to address at the outset of an internal investigation is to put in place an appropriate and robust governance structure, including who will have day-to-day management of the investigation and whom they will report to. The structure chosen will vary depending on the company and the issue.

Day-to-day management of the investigation is often given to the internal legal or compliance team, who will, therefore, likely be the 'client' for the purposes of instructing external legal counsel, with a consequent effect on the analysis of if and when legal advice and litigation privilege may arise. In any case, it will be important for potentially implicated individuals to be excluded from the investigation team, which should be kept under review in case additional individuals are implicated as a result of information that comes to light during the investigation. Where external advisers have been brought in to conduct an independent review, it may also be appropriate to limit the ability of the client to instruct or influence the review beyond clearly defined parameters, to preserve this independence. Further, if the issue under investigation arose as a result of whistleblowing, it will be important to bear in mind the rights of the whistleblower when designing the governance structure, particularly if the whistleblower has requested anonymity.

See Chapter 36 on privilege

See Chapter 19 on whistleblowing

The question of whom the investigation team will report to will often be determined by a company's existing corporate governance structure and framework of delegated authorities, and it is common for the investigation team to report to the board as a whole or the audit committee. However, in certain cases the company may choose to constitute a specific review body, such as a special subcommittee of the board or a panel of senior employees and external advisers. In such cases, the terms of reference of this body will need to be clearly defined, including what matters are to be referred to it, what powers it holds and how it is to interact with existing governance bodies in the company.

Where, as is common, the issue involves subsidiaries (some of which may not be wholly owned), it may be necessary to consider and reflect corporate separateness in the governance structure, such as reporting to the boards of those subsidiaries.

Whatever governance structures are established, it will be important to keep them under review and be able to amend them if new issues arise.

© Law Business Research 2021

Scoping the investigation 5.5

A well-defined scope, reflected in written terms of reference and an investigation plan, helps to ensure that the objectives of the investigation are clear and to avoid a wide-ranging, unfocused investigation, with consequent wastage of time, resources and cost. Clearly recording the scope, and its justification, will also better allow the investigation to be auditable if queries arise in the future.

A number of factors will affect the scope of the investigation. A narrow scope can help to focus resources and reach a quicker conclusion, but it may risk missing informative context. A wider scope can help to demonstrate that the investigation has been comprehensive, but it will increase the costs and time of the investigation. The appropriate scope will be affected by the nature of the issues (including whether the company is facing the risk of criminal, regulatory or civil action), the time pressures (especially if the company is in a race against co-infringers to apply for leniency) and whether there are, or are likely to be, concurrent investigations by authorities.

Defining the scope will also include deciding what the final deliverables will be. In some cases the default – a written report of factual findings – will be considered necessary, even though there is a risk that it may not be privileged. For example, in certain circumstances it may be advantageous to provide a written report to the authorities. The FCA Handbook states that a firm's willingness to volunteer the results of its own investigation, whether protected by legal privilege or otherwise, is welcomed by the FCA and is something the FCA may take into account when deciding what action to take.[18] Likewise, the DPA Code notes that co-operation (which is a public interest factor against prosecution) includes a company sharing its internal investigation report (including source documents) with the SFO; a point that has been highlighted by the courts in the DPA judgments handed down to date.[19] However, in other circumstances it may not be considered necessary or desirable to produce a potentially non-privileged written report. An alternative is for the investigation team to provide only oral updates on the factual findings. Other deliverables may include legal advice as to the company's exposure to litigation or investigation risk, self-reporting, employment law advice on disciplinary action against implicated employees, and mitigation and remediation proposals.

Companies must also assess whether to agree the scope of the internal investigation in advance with any authorities that are aware of the issue to be investigated. The benefits of doing so include potentially building co-operation

18 FCA Handbook, EG 3.11.2.

19 Deferred Prosecution Agreements Code of Practice, para. 2.8.2(i). Also see *Serious Fraud Office v. Rolls-Royce plc and Another* [2017] Lloyd's Rep FC 249, at para. 17; *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at para. 24; *Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435, at paras. 36 and 74; *Serious Fraud Office v. Güralp Systems Limited* [2020] Lloyd's Rep FC 90, at para. 27; S*erious Fraud Office v. Airline Services Limited* [2020] 10 WLUK 606, at para. 52; *Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep FC Plus 27, at para. 50.

© Law Business Research 2021

credit with the authorities, reducing the risk of the authorities later criticising the scope of the investigation and allowing the authorities an opportunity to express their preferences as to the final deliverables and the conduct of the investigation. The SFO in particular has expressed concerns about the potential for internal investigations to 'trample over the crime scene', and early engagement can help to avoid later criticism of the investigation team's actions.[20] The FCA Handbook states that if a firm anticipates that it will disclose a report of its internal investigation to the FCA, the potential use and benefit to be derived from the report will be greater if the FCA has had the chance to comment on its proposed scope and purpose.[21]

Finally, at the scoping stage it can be helpful to assess what external resources may be required during the investigation, which could include forensic accountants, asset tracers, private investigators, public relations firms and foreign counsel.

5.6 Document preservation, collection and review

In any internal investigation, it is critical to consider as early as possible the practicalities for the preservation, collection, review and analysis of relevant material. In its Corporate Co-operation Guidance, the SFO states that co-operation includes preserving available evidence and producing it to the SFO in an 'evidentially sound' format.[22] Any decisions regarding data preservation and review should be recorded in writing to preserve a clear audit and 'chain of custody' trail.

Although in the early stages of an investigation it may not be appropriate to conduct formal interviews, the investigation team may wish to consider conducting informal 'scoping interviews' to assist with scoping the investigation and identifying where relevant material might be stored. Care should be taken, given the preference of a number of authorities that they be consulted prior to interviews (even those relating to the location of evidence) to avoid the possibility of criticism that the internal investigation might have tainted the recollection of witnesses.

5.6.1 Preservation

Document preservation is extremely important and must be addressed as early as possible. It can, in certain circumstances, be a criminal offence to destroy or dispose, or permit the destruction or disposal, of documents that may be relevant to an external investigation, and both the SFO and the FCA have brought prosecutions for such offences.[23]

---

20 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO (20 May 2015), available at https://www.sfo.gov.uk/2015/05/20/compliance-and-cooperation/.

21 FCA Handbook, EG 3.11.5.

22 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

23 Richard Kingston, Managing Director at Sweett Group plc, was convicted of offences contrary to s.2(16) Criminal Justice Act 1987 in December 2016, and in 2019–2020, the FCA brought a prosecution against Konstantin Vishnyak for offences under s.117(3) FSMA, of which Mr Vishnyak was acquitted at trial.

© Law Business Research 2021

An important first step in document preservation is to identify which 'custodians' might hold information relevant to the investigation and which other sources might yield relevant documents (including any third-party sources). The sources of potentially relevant material may include emails, other electronic documents, external storage devices, mobile phones, tablets, internet messaging and chatroom data, telephone recordings[24] and hard copies. Companies should also identify any material they are unable to access (such as private email accounts, messaging applications or social media), as the relevant authorities may have statutory powers that allow them to access these sources. In its Corporate Co-operation Guidance, the SFO has stated it will consider it a mark of co-operation for companies to alert the SFO if there are any such inaccessible sources.[25]

The pool of custodians is likely to be broader than just those implicated in the suspected misconduct and may also include individuals reporting to them, individuals they reported to, secretaries and assistants, individuals in other departments they interacted with, and third parties outside the organisation. In some investigations, wider business units or offices might also be relevant.

In general, a company will issue a hold notice (also known as a document retention or document preservation notice) to such individuals asking them to preserve all (and not alter, discard, delete or destroy any) materials (including hard copies) they may hold relevant to the investigation. Beforehand, however, the company should consider whether circulation of the hold notice risks tipping off individuals relevant to the investigation who might destroy documentation or otherwise frustrate the investigation. In its Corporate Co-operation Guidance, the SFO states that genuine co-operation is inconsistent with 'putting subjects on notice and creating a danger of tampering with evidence or testimony'.[26] Potential solutions to address this risk include delaying the circulation of the hold notice until potentially relevant documentation has been secured or carefully drafting the hold notice so that it does not reveal the specific circumstances or subject matter of the investigation (subject, however, to the data privacy considerations discussed below). When drafting a hold notice a company should also consider the risk of it leaking and listed companies should consider whether the description in the hold notice is inside information.

Companies should take care to keep a clear record of the recipients of hold notices, especially where they are not circulated centrally, but instead are cascaded via the reporting structures of the organisation. As part of this, companies may wish to ask recipients to acknowledge their receipt and understanding of the hold notice, though this can create an administrative burden and raises the possibility that a recipient may refuse to acknowledge receipt. A middle ground may involve requesting an email read-receipt instead.

24 The FCA Handbook (SYSC 10A.1) places obligations on regulated firms to record telephone conversations that relate to regulated activities in certain financial instruments.

25 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

26 ibid.

© Law Business Research 2021

In support of the hold notices (which are issued to, and place the burden of preservation on, the relevant individuals), companies should also consider what other steps they can take centrally to preserve relevant materials. This may include the suspension of regular document destruction processes, activating permanent email holds (preserving emails regardless of whether individuals delete emails from their inboxes), creating computer drive backups (so that if individuals delete data from a shared drive, it can be recovered), imaging custodians' devices and preventing the recall of hard-copy documents from archives without appropriate authorisation. As noted above, it is good practice to implement these before the circulation of the hold notice to reduce the risk of individuals deleting data.

Companies should also be alert to the possibility of relevant data being stored on legacy systems and take steps to ensure that such data remains accessible during the investigation.

When issuing hold notices or taking other steps to preserve relevant materials, companies should carefully consider the potential application of data privacy rules and appropriately document their consideration of data subjects' interests. Key considerations under Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR)) will include identifying a lawful basis under the GDPR for the preservation, ensuring appropriate transparency (so that, subject to certain exceptions, the data subjects are aware of the scope and purposes of the preservation), data minimisation (so that no more data is preserved than is necessary) and storage limitation (so that the data is not stored for longer than is necessary).

See Chapter 40 on data protection

5.6.2 Collection

Having preserved all potentially relevant materials, the next step is to identify what should be collected for review. This will usually be a smaller and more focused set of materials, and identifying them will involve assessing where the materials relevant to the investigation are most likely to be found, keeping in mind the scope of the investigation.

Depending on the circumstances of the investigation, it may be desirable to instruct an external forensic services provider to collect the data. This will be especially important in the criminal context where issues relating to the forensic integrity of the underlying data and chain of custody are key.

The company will need to consider whether to notify the affected individuals of the data collection. This will depend, among other things, on the terms of any applicable data privacy policies at the company and the likelihood that giving notice may result in individuals destroying documents or otherwise frustrating the investigation. In certain circumstances, express consent may be required from employees, especially if prescribed by data privacy laws or if the employees use their own devices.

See Chapter 40 on data protection

It will also be necessary to consider the application of data privacy rules to the collection more generally. In particular, requirements to minimise the data collected can require the use of date range and keyword search terms (even before the data is ingested into a review platform) and principle of integrity

© Law Business Research 2021

and confidentiality may require the data to be stored securely and to be accessible only with appropriate authorisation.

Review 5.6.3

Having collected the data, in all but the smallest reviews, it is advisable to upload it to a document-review platform. This allows for easier searching, review and management of the data and will create an audit trail if questions arise in relation to specific documents.

The next stage will be to assess the appropriate searching criteria to help narrow the scope of the review and identify the most relevant documents. Available tools include applying date range, custodian and data source filters, and identifying relevant keyword search terms. If the timing allows, there are significant benefits to testing the potential searching criteria and refining them before starting the full review. There are also significant benefits to considering the appropriate type of data de-duplication to conduct.

Increasingly, vendors are offering technology-assisted analytics and technology-assisted review, in which the review software identifies links between documents or learns from initial reviewer coding decisions to identify similarly relevant documents from the remaining data set, so they can be brought to the attention of the review team sooner, or even automatically coded. The utility of this technology will, however, depend significantly on the quality of the initial 'seed set' of coding decisions and the complexity of the issues under review.

In any case, it is common to structure the review around a series of 'tiers', with an initial triage stage for relevancy, followed by second and potentially third-tier reviews by more senior individuals to focus the set and apply more complex coding. First-tier and even second-tier reviews are often outsourced to specialist document review service providers, which can free resource within the investigation team to concentrate on management of the review and other elements of the investigation.

To ensure accuracy and consistency of coding, it will be necessary to produce document review protocols and accompanying coding forms for each tier of the review, and to ensure the reviewers are fully briefed. It is also common to carry out regular quality control or calibration sessions with the reviewers, where they can ask questions of the senior team, and to set up a process for the rapid escalation to the senior team of key documents identified during the review.

In drafting the document review protocols and coding forms, it will be important to consider how the internal review may interact with any existing or potential parallel external investigation. In particular, if there is a possibility that relevant documents may be produced to an authority, there may be benefit in asking reviewers to code for privilege, data privacy, bank confidentiality and other jurisdiction-specific issues.

Documents located in multiple jurisdictions 5.6.4

Particular complexities can arise where documents, or other data, relevant to the internal investigation are located in other jurisdictions (including where

© Law Business Research 2021

data is hosted on cloud-based or group-wide servers that might be physically located overseas).

It will often be necessary to get local data privacy advice before preserving and collecting data held overseas, including on whether and how the data may be transferred to the jurisdiction where the review is taking place. If transfer of the data is not permissible, it may be necessary to conduct a local review within the foreign jurisdiction.

There are also wider strategic considerations to bear in mind before deciding to collect and transfer data from other jurisdictions. In particular, consideration should be given to the risk of voluntarily transferring documents into a jurisdiction so that they become available to authorities or civil litigation counterparties when they might not otherwise have been available to those third parties (although this should be balanced against the risk that in not collecting this data the company may be found to be unco-operative or frustrating the investigation).[27] Further, where data is held by a subsidiary, it may be necessary for the subsidiary to enter into co-operation and information-sharing agreements with its parent in relation to the investigation. It is common in these agreements (especially where the subsidiary is not wholly owned) for the subsidiary to retain a right of consent prior to its data being disclosed to any authority.

5.6.5 Importance of record-keeping

It is critical at all stages of an internal investigation to keep clear records of key decisions taken, including the drafting of detailed, auditable summaries of the methodology undertaken for data preservation, collection and review. It will also be important to maintain full chain of custody records for any originals of relevant documents, as well as for devices.

The FCA Handbook states that where a firm conducts an internal investigation, it will be 'very helpful' if the firm maintains a proper record of the enquiries made and interviews conducted.[28] Likewise, in its Corporate Co-operation Guidance, the SFO has emphasised the importance of maintaining an audit trail of the acquisition and handling of digital, hard-copy and financial material, and the potential need for companies to identify a person to provide a witness statement covering such issues.[29]

---

27 It is possible for authorities in the United Kingdom to request documents from authorities in other jurisdictions via diplomatic channels, including via mutual legal assistance treaties. Further, criminal law enforcement agencies in the United Kingdom have the ability to seek electronic data held by communications service providers located in the United States under the Crime (Overseas Production Orders) Act 2019, which aims to simplify and speed up the process of obtaining electronic data located abroad. As to the limitations on the territorial scope of SFO notices under s.2(3) Criminal Justice Act 1987, see *R (on the application of KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2.

28 FCA Handbook, EG 3.11.9.

29 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

© Law Business Research 2021

6

Beginning an Internal Investigation: The US Perspective

Bruce E Yannett and David Sarratt[1]

Introduction 6.1

The aim of this chapter is to provide the reader with useful tools to navigate the beginning of an internal investigation. Mistakes made in the initial phases of an investigation can have costly repercussions down the road, and, for this reason, it is important to consider all the relevant legal, commercial and logistical factors in making strategic decisions early on.

Assessing if an internal investigation is necessary 6.2

Information giving rise to the need for an internal investigation can come from a variety of sources, including customers, employees, whistleblowers, lawsuits, counterparties, news and social media, as well as from prosecutorial and regulatory authorities. Regulatory changes have created new incentives for individuals to come forward and report suspected wrongdoing. For example, the Sarbanes-Oxley Act of 2002 and its implementing rules require attorneys who appear and practise before the Securities and Exchange Commission (SEC) to report evidence of a material violation up the ladder to a company's chief legal officer and chief executive officer. The reporting obligation is not discharged until the attorney reasonably believes the company has provided an appropriate response.[2] Similar reporting obligations apply to issuers and auditors.[3]

When confronted with information – from whatever source – that the company or its employees may have engaged in serious misconduct, in-house counsel's first step is often to assess whether it would be in the company's

1 Bruce E Yannett and David Sarratt are partners at Debevoise & Plimpton LLP.

2 See Sarbanes-Oxley Act of 2002 § 307, 15 U.S.C. § 7245; 17 C.F.R. 205.3(b) 2021.

3 See Securities Exchange Act of 1934 § 10A, 15 U.S.C. § 78j-1.

© Law Business Research 2021

interest to conduct an internal investigation. Counsel will want to consider whether government authorities are already investigating, or are likely to investigate, the matter, whether civil litigation will follow and in what form, and the potential (or likely) need for remediation. Depending on the facts, counsel may also want to balance the costs of investigating and the potential disruption to normal business, as well as any potential reputational risk or commercial fallout.

In some instances, external legal obligations may require an investigation to be conducted. Board members and management, for example, have a fiduciary duty to protect the interests of the corporation and its shareholders, and in some cases that duty will include an obligation to investigate indications of serious misconduct at the company. An investigation may also be required in certain instances so that company executives can meet any affirmative certification obligations they have, whether under Sarbanes-Oxley or otherwise.

More often, however, counsel will want to conduct an investigation to make an informed decision about whether it is in the company's interest to self-report the matter to law enforcement or regulators. Over the past two decades, the United States Department of Justice (DOJ) has placed an increasing focus on self-reporting both in charging decisions and in the degree of co-operation credit that will be afforded to a company. To guide the charging decisions of its own attorneys, the DOJ has set out a number of factors that prosecutors should consider in determining whether to charge a business entity, including co-operation and voluntary disclosure, the adequacy of the corporation's compliance programmes, and any remedial actions or restitution undertaken.[4] The DOJ has expanded on these factors through subsequent directives.[5] In November 2019, the DOJ clarified that under its revised policy, a company seeking co-operation credit is expected to disclose 'all relevant facts known to it at the time of the disclosure'.[6] This clarification recognises that because 'a company may not be in a position to know all relevant facts at the time of a voluntary self-disclosure, especially where only preliminary investigative efforts have been possible', a full investigation is not required before disclosure, though a company should 'provide a fulsome disclosure' of the relevant

See Chapter 4 on self-reporting to authorities

4 See Holder Memorandum, Bringing Criminal Charges Against Corporations, Dep't of Justice, Dep. Att'y Gen. Eric Holder (16 Jun. 1999).

5 See Thompson Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Dep. Att'y Gen. Larry D Thompson (20 Jan. 2003); McCallum Memorandum, Waiver of Corporate Attorney–client and Work Product Protections, Dep't of Justice, Acting Dep. Att'y Gen. Robert D McCallum (21 Oct. 2005); McNulty Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Dep. Att'y Gen. Paul J McNulty (12 Dec. 2006); Filip Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Dep. Att'y Gen. Mark Filip (28 Aug. 2008); Yates Memorandum, Individual Accountability for Corporate Wrongdoing, Dep't of Justice, Dep. Att'y Gen. Sally Q Yates (9 Sep. 2015).

6 United States Department of Justice (DOJ), Justice Manual § 9-47.120 (updated Nov. 2019) (Justice Manual).

© Law Business Research 2021

facts known at the time.[7] Just two years later, the DOJ restored prior guidance mandating that this disclosure identify all individuals involved in the misconduct, not merely those who were 'substantially involved'.[8] Additionally, in 2016, the Fraud Section of the DOJ launched a 'Pilot Program' announcing even greater emphasis on voluntary self-reporting in deciding whether to charge or how to resolve corporate criminal matters.[9] The following year, this policy was formally implemented through the DOJ's revised Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, which was announced on 29 November 2017 and closely tracks the objectives of the Pilot Program, including the incentives for self-disclosure and co-operation with the DOJ's investigations.[10] The DOJ has since indicated that this policy will likely be extended, at least in practice, to cases that come before the Department involving other federal regulations beyond the FCPA.[11]

In light of these policies, for all practical purposes, an internal investigation is often necessary so that the company can identify what, if any, information should be disclosed to the DOJ, and whether co-operation credit is attainable.

---

7 Justice Manual § 9-47.120 n. 1. The revised policy also provides that a company must let the DOJ know 'where the company is aware of relevant evidence not in the company's possession'. For the purposes of determining the appropriate form of any resolution or prosecution, including any monetary penalties or compliance obligations contained in any corporate criminal resolution, the DOJ recently clarified that prosecutors should consider the corporation's 'timely completion of thorough investigations', as well as 'what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts'. DOJ, Evaluation of Corporate Compliance Programs 1, 6, 14 (updated Jun. 2020).

8 See Dep. Att'y Gen. Lisa O Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime (28 Oct. 2021), available at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

9 Leslie R Caldwell, Criminal Division Launches New FCPA Pilot Program (5 Apr. 2016) (noting that '[i]f a company opts not to self-disclose, it should do so understanding that in any eventual investigation that decision will result in a significantly different outcome than if the company had voluntarily disclosed the conduct to us').

10 See Dep. Att'y Gen. Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, U.S. Dep't of Justice (29 Nov. 2017); Justice Manual § 9-47.120 (updated Nov. 2019). The DOJ and Securities and Exchange Commission (SEC) have since noted that they both 'place a high premium on self-reporting, along with cooperation and remedial efforts, in determining the appropriate resolution of FCPA matters'. DOJ and SEC, 'A Resource Guide to the US Foreign Corrupt Practices Act' (2d ed. 2020). For example, the DOJ recently declined to prosecute the World Acceptance Corporation for FCPA violations, citing the company's 'prompt, voluntary self-disclosure of the misconduct' and its 'full and proactive cooperation'. Letter Declining to Prosecute World Acceptance Corp. (5 Aug. 2020).

11 See Head of the Criminal Division John Cronan and Chief of the Securities and Financial Fraud Unit Benjamin Singer Deliver Remarks at the ABA's 32nd Annual National Institute on White Collar Crime (1 Mar. 2018); Letter Declining to Prosecute Barclays PLC (28 Feb. 2018), stating: 'The Department's decision to close its investigation of this matter is based on a number of factors, including . . . Barclays' timely, voluntary self-disclosure'.

© Law Business Research 2021

This, however, may be a false dilemma as, in many instances, a corporation's co-operation can be the most significant determining factor in how the DOJ resolves a case, including the amount of any penalty.[12]

Many regulatory agencies have likewise increasingly come to expect companies to perform a robust internal investigation of any potential legal or regulatory violations and to report such violations to the agency. For example, the Consumer Financial Protection Bureau (CFPB) has stated that 'responsible conduct' – namely proactive self-policing for potential violations, prompt self-reporting of identified violations, complete remediation of resulting harm and co-operation with the CFPB – would influence the CFPB's resolution of an enforcement investigation.[13] Similarly, the US Department of Treasury Office of Foreign Assets Control specifically provides companies with mitigation credit of 50 per cent off its base penalty amounts for voluntary disclosures and further mitigation for co-operation.[14] The SEC similarly identifies '[s]elf-policing, self-reporting, remediation and cooperation with law enforcement authorities' as the primary factors it will consider in determining an appropriate resolution.[15]

Even apart from legal considerations, business and reputational concerns alone may provide grounds for conducting an internal investigation. Indeed, counsel will often need to have a baseline understanding of the underlying facts, and an informed sense of whether there is any substance to the allegations of misconduct, to make a reasonable assessment of the potential business and legal consequences and the need for corrective action. Commencing a thorough internal inquiry will often also be important to any related public relations efforts, and will be critical to maintaining the company's credibility with its customers, business partners and other affected individuals.[16]

12 See U.S.S.G. § 8C2.5(g), cmt. 13 (2018).

13 CFPB Bulletin 2013-06 app. A n. 6, Responsible Business Conduct (25 Jun. 2013).

14 31 C.F.R. Part 501, Economic Sanctions Enforcement Guidelines (9 Nov. 2009).

15 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Release No. 34-44969 (23 Oct. 2001) (Seaboard Report). For example, the SEC accepted Gulfport Energy Corporation's settlement offer and declined to pursue a civil penalty because of the company's prompt remedial acts and significant co-operation with the SEC. Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, Release No. 91196 (24 Feb. 2021).

16 In rare circumstances, some facts will be so clearly unlawful on their face (e.g., if an employee is providing clearly and materially false information to investors) that the company should consider notifying the relevant law enforcement or regulatory authorities even before conducting a complete internal investigation, particularly where time is of the essence and, if appropriate, continue with the internal investigation in parallel.

© Law Business Research 2021

Identifying the client 6.3

Once the company decides to commence an internal investigation, the next step is to determine who will conduct the investigation and for what specific client within the organisation. In large organisations, particularly those with multiple subsidiaries across the globe, counsel should think strategically about how to structure the investigation: where to locate the attorney–client relationship, to whom the investigating attorneys should report, and who will be making key decisions as the investigation proceeds. In making these decisions, counsel should consider what relationships will best protect the integrity and confidentiality of the investigation, the location and custody of relevant documents, and the overall aims of the investigation over the short and long term.

In some circumstances, counsel may also want to consider whether the investigation should be conducted on behalf of the board (or its subcommittee), with counsel reporting to and being directed by the board, rather than by management. In a shareholder derivative suit, having the board direct the investigation will be the norm, both because the conduct of management will often be at issue and so that the investigation will not be subject to the derivative-claim exception to the attorney–client privilege recognised in some jurisdictions. The board may also be best suited to lead an investigation when the allegations are particularly serious or could have serious consequences for the company, when the allegations concern the actions of senior management, or when reputational or other concerns require that the investigation be conducted independently of management. Making that decision in any particular case will depend heavily on the specific facts involved, the company's business and position in the marketplace, the relationship dynamics at the company and the overall goals of the investigation.

See Chapter 37 on privilege

Whatever decision is made, it is important that the company clearly document who the client is, and the reporting and oversight structure for the investigation.

Control of the investigation: in-house or external counsel 6.4

Although routine matters can often be handled by in-house counsel, an outside firm should ordinarily conduct the investigation where the potential misconduct could produce significant adverse legal or commercial consequences for the company. Though internal investigations can be expensive and time-consuming, these concerns often pale in comparison to the possible legal, financial and reputational risks faced by the company, as well as the need to demonstrate independence. Hiring external counsel allows for a clearer application of attorney–client privilege to the communications and work-product of the outside firm, especially where corporation counsel has both business and legal functions. Often, both commercial and legal concerns can precipitate an internal investigation, so using external counsel can decrease the risk of

© Law Business Research 2021

inadvertently waiving privilege.[17] External counsel also brings expertise, experience and resources to support the company in challenging situations that are unlikely to arise with much frequency at any particular company.

Depending on the circumstances, in-house counsel may want to consider using external counsel that is not the company's usual firm.[18] Bringing in a separate firm that is less familiar with the company's business, of course, will often involve additional time and expense. Whether this step is justified in a particular case will depend on the sensitivity and significance of the investigation, the level of management implicated in the conduct, the need for perceived independence of the investigation, and the attitude of potentially relevant regulators who may be assessing the quality and results of the investigation in considering whether the company deserves credit for co-operation.

6.5 Determining the scope of the investigation

The importance of clarifying the investigation's scope and purpose at the outset cannot be overstated. First, a well-defined and memorialised purpose can help establish the legitimacy of privilege claims over attorney–client communications and work-product produced in the course of the investigation; the claim to attorney–client privilege is likely to be much stronger if an independent investigation has been commenced or litigation is reasonably in contemplation.

See Chapter 37 on privilege

Additionally, defining the investigation's purpose can impose a welcome discipline and accountability on the investigators themselves. Corporate counsel are quite familiar with the tangents that can cause an investigation to become rudderless and wasteful. As explained below, a short period of preliminary investigation can often be helpful in defining a purpose and scope to the investigation that is reasonably clear and realistic, while identifying key uncertainties and inflection points to come. In defining the scope of the investigation, it can also be valuable to consider how quickly the information is needed, whether based on requests from the government or internal time pressures.

6.5.1 Key documents and scoping interviews

Most investigations will begin with counsel's review of a handful of critical documents that are at the heart of the information triggering the need for the

17 See, e.g., *United States v. Ruehle*, 583 F.3d 600, 606-12 (9th Cir. 2009) (statements made for the purpose of disclosure to outside auditors not privileged). In the United States, however, investigations conducted solely by in-house counsel may fall within the scope of the attorney–client privilege if they are carefully conducted. See, e.g., *In re Kellogg, Brown & Root, Inc.*, 756 F.3d 754, 758 (D.C. Cir. 2014) ('*Upjohn* does not hold or imply that the involvement of outside counsel is a necessary predicate for the privilege to apply.'). The extent to which an investigation conducted by in-house counsel outside the United States would be protected by privilege varies widely by jurisdiction.

18 See *In re John Doe Corp.*, 675 F.2d 482, 491 (2d Cir. 1982) (recognising that when corporate counsel finds evidence of criminality protected under *Upjohn* 'the wiser course may be to hire counsel with no other connection to the corporation to conduct investigations').

© Law Business Research 2021

investigation. In many instances, the documents themselves, rather than individuals, may have alerted the company to alleged wrongdoing and precipitated the need for an investigation. In almost every case, however, conducting a small number of initial scoping interviews will be a useful way for the investigators to focus in quickly on the truly important material.

Identifying the most useful individuals to speak with in these scoping conversations can be delicate, as investigators seek to strike a balance between speaking with individuals who are knowledgeable about the issue at hand but who are sufficiently removed from the potential misconduct that they can safely be viewed as reliable in terms of setting the scope and maintaining the confidentiality of the investigation. Of course, interviewing an employee at an early stage, without the benefit of a complete set facts or documents, could result in incomplete information and the need for a further interview.

One logical place for external counsel to start is to thoroughly debrief the in-house legal team and, potentially, the individual or individuals who brought the issue to the attention of the organisation. These interviews can serve to identify key custodians, the nature and volume of relevant documents, the ways documents are stored, and who has access to them. If there is an obvious investigation target, interviewing that individual in the initial stages may be more efficient, but this must be weighed against other strategic considerations, including alerting the target to the focus of the investigation and compromising the investigation later on. The timing and structure of these initial discussions may also be influenced by external deadlines or other business considerations involved in the review.

Identifying necessary partners 6.5.2

Another early consideration for counsel is what outside investigative partners may be needed. These can range from technical subject-matter experts to local counsel in foreign jurisdictions to data processing and hosting services to forensic accountants. Counsel ordinarily will want to interview a number of firms in deciding which vendors to use, and the discussions can sometimes yield helpful insight into the size of the tasks ahead, likely costs, potential alternative strategies and timing. Engaging these third parties at the outset of the investigation – even if their work is not needed immediately – will often be valuable in defining the scope and methods of the investigation. As noted above, given the consideration of attorney–client privilege, generally external counsel will retain the third-party vendors on behalf of the company so that their work and work-product is undertaken on the instruction of external counsel in anticipation of litigation and thereby covered by privilege and attorney work-product protections.

Developing a work plan 6.5.3

Once the investigating attorney has identified the subject matter of the investigation (the who, what, when and where), the scope and the purpose of the investigation and a concrete plan for carrying it out should ordinarily be

© Law Business Research 2021

memorialised by external counsel in a written work plan. This type of memorandum allows for client input on the investigative process, gives in-house counsel clear expectations about how the investigation will progress, and provides investigating attorneys with a benchmark for strategic judgements as the investigation moves forward. It can also serve as a useful tool for dividing responsibilities among the investigating attorneys and tracking progress toward key investigative goals. Keep in mind that the work plan may be a document that the company decides to share with the criminal or regulatory authorities and should be drafted accordingly.

In building the work plan, counsel should consider the time frame and geographical range of the inquiry, as well as which entities of the company (e.g., subsidiaries, affiliates, departments) will be covered and, if applicable, the rationale for not covering other entities at this stage. The memorandum should clearly set forth the subject matter under investigation and, to the extent possible, (1) what company documents will be retrieved (and by whom), (2) how data will be processed (and by whom), and (3) how documents will be reviewed (and by whom). In collecting, reviewing and preserving documents, the investigating attorney should take into account any data privacy concerns that may arise.

Where possible, the work plan should list any interviews that have been or will be conducted, or at least the categories of people to be interviewed. To the extent there is a rationale for interviewing some individuals and not others, it should be stated. Likewise, if the involvement of other third parties, such as forensic accountants and industry experts, is foreseeable, the document should describe the scope of their expected engagement.

The work plan should also set a rough schedule for key deliverables in the investigation, and at least tentatively identify the form that the ultimate work-product will take. In particular, it is useful to know at the outset of an investigation whether the preparation of a written investigative report will be useful and in the company's interest, or whether an oral presentation of findings to management or the board would be preferable. A written report will most often be advisable when the company believes providing the report to a third party or to the public will be beneficial, whether for reputational, business or legal reasons. In most other cases, an oral report will often serve the client's interests just as well without creating a risk of inadvertent or compelled disclosure.

Finally, the work plan should be flexible. Although careful planning is always beneficial, investigations in the real world are not scripted affairs. The investigative team will have to adapt to new information and challenges as the investigation progresses, and the work plan should lay out a process for making those decisions – particularly in terms of who should be consulted and who should approve decisions – before the investigative team moves in a new direction not contemplated by the plan.

Certain investigations may implicate the general counsel or other members of senior management in alleged misconduct. In that circumstance, the

© Law Business Research 2021

investigating attorneys should report to the board (or a designated member or committee of the board) or to a senior executive who has no involvement in the facts at issue and who does not report to any member of management whose conduct may be under review.

Document preservation, collection and review 6.6

Preservation 6.6.1

As soon as possible after learning of potential misconduct, the in-house attorney should implement a litigation hold and disseminate a document preservation notice to prevent the intentional or inadvertent destruction of relevant documents and material. In fashioning the document retention policy, it is ordinarily advisable to err on the side of overbreadth, at least at the beginning when the extent of any potential wrongdoing and the relevant actors are unknown. This is critical. Failure to successfully preserve relevant material could be viewed as a dereliction of the attorney's duties and, in some cases, as obstruction of justice.

In issuing preservation or 'hold' notices, the investigating attorneys should consider who should receive these notices (including the IT and records departments), what types of documents and data should be included, and how the investigation should be described. Where notices are sent to different jurisdictions, the investigating attorney may need to consider providing translations as well as addressing data privacy restrictions. The attorney implementing the litigation hold should record the distribution of notices and, where extra caution is warranted, have employees sign and return a copy of the notice or electronically acknowledge receipt so as to create a record. If the company has received a subpoena from law enforcement relating to the subject matter of the investigation, the subpoena will define the minimum universe of documents that require preservation, but counsel should consider whether additional material should be preserved for purposes of the internal investigation or otherwise.

The investigating attorneys should consult with the company's records management department to preserve any hard-copy files, including those stored off-site in archives. The investigating attorney should also instruct the IT department to suspend any normal data destruction practices and to create and maintain a list of the relevant sources of data. Such sources may include documents maintained on the company's servers and employees' hard drives, emails saved on exchange servers, data held on employees' home computers, and data saved on employees' work-issued mobile and electronic devices – the collection of which may require additional considerations when employees have been furloughed or are working remotely. In recent years, regulators have been increasingly focused, not just on collecting and preserving email, but also on collecting and preserving text messages and other communications stored

© Law Business Research 2021

on mobile and other electronic devices.[19] To the greatest extent possible, the company should take steps on its own to preserve this electronic data rather than relying on individual employees to preserve their own documents. The company should also take steps to prevent individuals from destroying or altering potentially relevant data. In some cases the facts will warrant proactive data capturing steps, including forensic images of employees' laptops, desktops or mobile devices. Document custodians should be designated as soon as the investigating attorneys reasonably believe such individuals may possess documents relevant to the investigation.

It bears mention that sometimes the document collection process itself can come under scrutiny, particularly if authorities come to believe that relevant (and potentially damaging) documents may have been destroyed. In some extreme cases, someone with first-hand knowledge of the investigation may be called to provide sworn testimony in a deposition or in court. Attorneys should plan and document the collection process with this worst-case scenario in mind, and make clear to their clients the importance of treating the collection process – sometimes viewed as an administrative chore – with serious care and attention.

6.6.2 Collection

Once preservation measures have been implemented, the investigation can turn its attention to the collection of documents. Almost all investigations require judgement calls to be made on the scope of which documents to collect and from whom, including whether the investigation can be accomplished in whole or in part through collection within the company or, instead, requires collection from third parties. Company policies (e.g., codes of conduct) and local employment law also may impose limitations on the collection process. If the investigation contemplates the collection of personal health information, counsel should ensure that all data collection comports with the requirements of the Health Insurance Portability and Accountability Act of 1996. In such circumstances, counsel should take appropriate measures to safeguard personal health data, including assessing whether entering into a business associate contract is appropriate.[20] By the same token, counsel should ensure that any other personally identifiable information collected as part of the investigation is similarly flagged during review and appropriately safeguarded.

---

19 For example, for a company to receive full credit for timely and appropriate remediation in FCPA matters, the DOJ expects companies to implement 'appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations.' Justice Manual § 9-47.120 (updated Nov. 2019).

20 The Rules under the Health Insurance Portability and Accountability Act of 1996 generally require that covered entities enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. See 45 C.F.R. Parts 160 and 164.

© Law Business Research 2021

For electronic data, the process of collecting data will often coincide with preserving it. Counsel should make sure that forensic copies of all relevant electronic data (including metadata) have been copied to a secure location, preferably with at least one backup maintained on a separate system. The data will then need to be loaded into a review platform for review. Evidence that has been collected in paper form will often be most easily reviewed by digitising it and loading it into the same review platform as the electronic documents that have been collected. The data vendor retained by the investigating counsel will provide the collection and hosting support to the company.

As with the preservation process, the steps taken in collecting documents should be recorded. In instances where requested documents cannot be located, the search efforts and results should also be documented.

Review 6.6.3

Regarding the review of the documents, the investigating attorneys should carefully consider how best to manage the volume and formatting of documents. Outside vendors are a useful resource for these matters, and consulting with them early can often save time and money.

Where there is a large volume of documents to be searched, the key objective is to locate the responsive documents quickly and efficiently. Search terms should be broad enough to include responsive materials, but narrow enough not to bog down review teams with a large proportion of unnecessary documents. To the extent certain custodians or groups of documents are more likely to contain relevant content, their review should be prioritised.

In recent years, great advances have been made in the use of predictive coding in e-discovery to more quickly identify relevant documents and reduce the number of non-responsive documents that need to be individually reviewed. In our experience, the judicious use of predictive coding technologies is increasingly acceptable to regulators and prosecutors in the right context, so long as the specific methodologies and rationale for using those tools are clearly discussed with the authorities at the outset.[21] Even in cases where a full human review of a document population is contemplated or required, predictive coding can be a useful tool for internal investigators in locating the most relevant documents quickly, before the full review is complete.

Taking these considerations into account, the investigating attorneys should draft a document review protocol that sets forth in as much detail as possible the purpose of the review, the responsive issues, and how documents should be tagged or marked. Devising the system of tags and codes is a critical step.

21 In the civil context, 'it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it'. *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 127 (S.D.N.Y. 2015). The DOJ has supported the use of technology-assisted review as a timely and cost-effective way to accomplish a document review in a criminal matter. See *Cohen v. United States*, No. 18-MJ-3161 (S.D.N.Y. Apr. 26, 2018), ECF No. 28.

© Law Business Research 2021

Counsel should give careful consideration to how they may want to sort the data as the investigation progresses and devise codes that will make that work efficient. On the other hand, counsel should take care not to include so many codes that the review will be unduly slowed or overly confusing to reviewers.

If the need to produce documents to outside parties is likely, responsive documents should be reviewed to see if they are privileged and, if so, which privilege would apply. Disclosure of privileged material to a third party, even the government, can in some instances constitute a waiver of privilege, although steps can be taken to limit the scope of such a waiver.

See Chapter 37 on privilege

In the context of an investigation, gathering material is a dynamic process. Discovery of documents will often require follow-up interviews, and information gleaned in interviews may reveal the need for additional search terms or custodians. Documents retrieved from one custodian may reveal that a previously unknown custodian may have responsive material. The document preservation notice and review protocol should be updated as needed throughout the course of the investigation as this information comes to light.

6.7 Documents located abroad

When documents are located in jurisdictions outside the United States, the first step is to look at the relevant country's data privacy and bank secrecy laws (or whether blocking statutes or state secrecy laws are implicated), many of which may seem counter-intuitive to US practitioners.[22] In the European Union, for instance, employees' personal data can only be collected and processed under certain conditions, and law firms and their clients must protect this data from misuse and respect certain rights of the individual data owners.[23] These requirements and the penalties for non-compliance have been heightened by the recent implementation of the General Data Protection Regulation, which superseded the Data Protection Directive governing data privacy and applies directly throughout the European Economic Area. Some countries also have procedural requirements (e.g., notification to a works council) that govern the processing, transfer, storage, maintenance and access to documents.[24] Given

See Chapter 40 on data protection

22 In some cases, data privacy regimes can also apply to documents located within the United States if the data resides there in connection with the activities of a non-US entity. This is true, for example, of the European Union General Data Protection Regulation, which has extraterritorial effect in certain circumstances.

23 See the EU General Data Protection Regulation adopted in April 2016, which came into effect on 25 May 2018 and superseded the EU Data Protection Directive (Directive 95/46/EC). Other notable data privacy laws include Brazil: General Personal Data Protection Law (Law 13,709/2018); China: the Personal Information Protection Law (Chairman's Order No. 91); Hong Kong: Personal Data (Privacy) Ordinance (Cap 486); Japan: the Act on the Protection of Personal Information (Law No. 57 of 2003); and Russia: the Russian Federal Law 'On Personal Data' (No. 152-FZ).

24 See, e.g., Articles 91, 96 and 96a of the Austrian Labour Constitution Act (*Arbeitsverfassungsgesetz* (ArbVG)).

© Law Business Research 2021

the heightened scrutiny surrounding personal information, counsel should take care to collect and store only what the investigation requires, and consider whether any special arrangements, such as a cross-border data transfer agreement, would help mitigate collateral risk.

In the past, corporate counsel has sometimes relied on these foreign laws to avoid producing documents located abroad to US authorities. Recently, DOJ officials have expressed increasing scepticism toward explanations that documents cannot be provided to the DOJ in the United States because of data privacy restrictions, and, by virtue of handling many cases implicating foreign laws, have themselves become knowledgeable about their limitations and exceptions. In the DOJ's view:

> *Corporations are often too quick to claim that they cannot retrieve overseas documents, emails or other evidence regarding individuals due to foreign data privacy laws. . . . A company that tries to hide culpable individuals or otherwise available evidence behind inaccurately expansive interpretations of foreign data protection laws places its cooperation credit at great risk.*[25]

In 2015, Leslie Caldwell, then head of the Criminal Division at the DOJ, stated that while 'some foreign data privacy laws may limit or prohibit the disclosure of certain types of data or information', the DOJ nonetheless will challenge what it perceives to be 'unfounded reliance on these laws' and encouraged companies to refrain from 'making broad "knee jerk" claims that large categories of information are protected from disclosure'.[26] The following year, Caldwell reiterated that the DOJ was leveraging its relationships with foreign enforcement partners 'to obtain information when non-cooperative companies make invalid assertions about particular data privacy laws in an effort to shield themselves from [DOJ] investigations'.[27] The DOJ's FCPA Corporate Enforcement Policy now provides that '[w]here a company claims that disclosure of overseas documents is prohibited due to data privacy, blocking statutes, or other reasons related to foreign law, the company bears the burden of establishing the prohibition', and that 'a company should work diligently to identify all available legal

25 Remarks by Principal Deputy Assistant Attorney General for the Criminal Division Marshall L Miller at the GIR Live conference, New York, 17 Sep. 2014, available at https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller.

26 Remarks by Assistant Attorney General Leslie R Caldwell at the Compliance Week Conference (19 May 2015), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-compliance-week-conference.

27 Remarks by Assistant Attorney General Leslie R Caldwell at the American Bar Association's 30th Annual National Institute on White Collar Crime (4 Mar. 2016), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-american-bar-association-s-30th.

© Law Business Research 2021

bases to provide such documents'.[28] As the then Deputy Assistant Attorney General Matt Miner stated in 2019, the DOJ's 'expectation is that a cooperating company will work to identify all available legal means to provide such evidence and, if the company determines that it is unable to provide such information, [the DOJ] will expect a detailed explanation as to why'.[29]

This is not to say that companies should disregard or be cavalier with foreign data privacy laws. But counsel should look for solutions to this issue. Where potential strategies exist – even creative ones – for obtaining relevant documents that are located abroad, United States authorities have clearly indicated they expect companies to do so to receive co-operation credit. This will almost always require coordination with skilled counsel in the relevant jurisdiction where the documents are located.

28 Justice Manual § 9-47.120 (updated Nov. 2019).

29 Remarks by Deputy Assistant Attorney General Matt Miner at the American Bar Association, Criminal Justice Section Third Global White Collar Crime Institute Conference (27 Jun. 2019), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matt-miner-delivers-remarks-american-bar-association.

© Law Business Research 2021

7

Witness Interviews in Internal Investigations: The UK Perspective

Caroline Day and Louise Hodges[1]

Introduction 7.1

Witness interviews are a key part of most corporate investigations. While documentary evidence can provide the underlying facts of a case, it is often the accounts given by witnesses that deliver the context and detail of what has happened. They can provide vital background information, shed light on the motivations of those involved and allow for an individual's credibility to be assessed. However, the timing, preparation, record-taking, content and use of the interviews need careful consideration.

Witness interviews can serve a number of purposes in the context of a corporate investigation, including:

- to scope the investigation;
- to understand the facts and issues;
- to understand accountability and defences; and
- to assess the credibility of individuals and their accounts.

Interviews in this context can present particular difficulties because of the myriad employment, criminal, civil and regulatory issues that can arise, and the fact that the interests of the company and the witness are often not aligned. These interviews are typically conducted confidentially and can be premised on a need to maintain legal privilege and the duty of confidence owed between an employer and employee. This can often be at odds with the expectations of some authorities for the company to provide details of the witnesses' accounts.

1 Caroline Day and Louise Hodges are partners at Kingsley Napley LLP. The authors would like to thank Will Hayes, a senior associate at Kingsley Napley LLP, for assistance with this chapter.

© Law Business Research 2021

There is often a tension between a company's right to conduct its own enquiries into allegations of wrongdoing, including interviewing its employees, and the suggestion by the authorities that its enquiries could (depending on how they are conducted) be detrimental to a criminal or regulatory investigation. In addition, the position surrounding legal privilege in the context of witness interviews has become more complex over the past few years following a number of court judgments.

This chapter explores these issues, considers the practices that can be adopted when conducting interviews and highlights some of the benefits and risks of these different approaches. It considers the preparation and formalities that may be required for witness interviews in the United Kingdom, and identifies particular complexities that can arise in global investigations when multiple jurisdictions are involved.

7.2 Types of interviews

Broadly, witness interviews in corporate investigations can be split into two categories: preliminary or scoping interviews, and substantive interviews. Generally, they should be distinguished from any employment or disciplinary interviews.

Preliminary or scoping interviews may be appropriate at the outset of an investigation to seek background information, identify further sources of evidence, obtain a quick understanding and provide context to an allegation. These interviews will generally take place at the start of the investigation and, depending on the specific circumstances, may take place before any firm view has been reached on the terms of reference or extent of material that will be reviewed. They are more likely to be conducted with employees who may have knowledge of matters under investigation but are not at direct risk of any criticism. It may also be necessary to undertake interviews with whistleblowers at this stage.

See Chapter 19 on whistleblowers

Substantive interviews will generally take place after most, if not all, the relevant material has been reviewed. The purpose is to obtain a detailed understanding of what went on, to provide explanations of key documents in the case and, if necessary, to test the account given. These interviews will often be used to inform an understanding of any individual and corporate liability and any defences. The timing is important and can depend on a number of factors, including the available evidence, whether the authorities are already involved and whether civil and criminal proceedings are contemplated.

More recently, there has been a rise in internal investigation interviews being conducted remotely, given advances in technology and the need for remote working.

Where interviews are conducted remotely, it is important to ensure that the integrity and effectiveness of the investigation is maintained. Measures should be put in place to ensure that interviews are conducted confidentially and to limit the risk of any breach of this, whether intentional or inadvertent.

© Law Business Research 2021

Deciding whether authorities should be consulted 7.3

The decision about whether to consult the authorities in advance of a witness interview is not dictated by statute, and, in general terms, a company may manage its internal affairs and make enquiries as it sees fit. The decision often rests on whether there is an implicit obligation on the company to notify the authorities under its regulatory reporting regime, whether it is in the interests of the company to co-operate with the authorities by notifying them of any forthcoming interviews and the extent to which the authorities are already involved.

Regulated firms may be obliged to report a violation or allegation of wrongdoing. For example, the Solicitors Regulatory Authority's (SRA) Code of Conduct requires a law firm to report promptly any facts or matters that it reasonably believes are capable of amounting to a serious breach of the SRA's standards or requirements of which they are aware, to report any material change about the firm and to co-operate with the SRA and provide full and accurate explanations, information and documentation in response to any requests or requirements.[2] Accountants may hold similar obligations under the requirements of their regulators. There are reporting requirements under the Listing Rules for those companies admitted to trading on a regulated market,[3] and those in the regulated sector are required to submit a suspicious activity report if they know or suspect (or have reasonable grounds for knowing or suspecting) that another person is engaging in money laundering or terrorist financing.[4]

Financial institutions regulated by the UK Financial Conduct Authority (FCA) must under Principle 11 of the FCA's Principles for Businesses act in an open and co-operative way and disclose anything relating to the firm of which the regulator would reasonably expect notice.[5] Firms that are dual-regulated by the FCA and Prudential Regulation Authority (PRA) have equivalent obligations under Fundamental Rule 7 of the PRA's Fundamental Rules.[6] The FCA's expectations under Principle 11 extend to requiring a firm to consider notifying it of a decision to investigate conduct concerns at the earliest opportunity and it has previously suggested self-reporting is the bare minimum that is required, and that firms should discuss the scope of its investigation with the FCA as early as possible.[7] Furthermore, the FCA's Enforcement Guide sets out[8] that, in

2 Solicitors Regulatory Authority (SRA) Code of Conduct for Firms, Chapter 3 . See also the SRA's Guidance Reporting and notification obligations, published on 25 November 2019: https://www.sra.org.uk/solicitors/guidance/reporting-notification-obligations/.

3 Also see Prospectus Rules and Disclosure and Transparency Rules.

4 Proceeds of Crime Act 2002, Part 7 and Terrorism Act 2000, Part 3.

5 Also see FCA Supervision Manual 15.

6 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/new-bank/Fundamentalruleprinciples.

7 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA, at the Pinsent Masons Regulatory Conference 2015, 5 November 2015.

8 At para. 3.11.7.

© Law Business Research 2021

certain circumstances, the FCA may prefer that a firm does not commission its own investigation if that in itself could be damaging to an FCA investigation, particularly in the case of criminal investigations, where alerting the suspects could have adverse consequences; the guide states that firms are encouraged be alive to the possibility that their own investigations could prejudice or hinder a subsequent FCA investigation, and, if in doubt, to discuss this with the FCA.

A firm should consider its regulatory obligations when assessing if, and when, to consult the FCA regarding any proposed witness interviews. It should ensure it does not take steps that might prejudice or hinder a subsequent FCA investigation.[9]

The Serious Fraud Office (SFO) has similarly acknowledged that there are good and proper reasons for a company to carry out its own investigation,[10] noting the potential dangers of an internal investigation 'churning up the crime scene', which could include the taking of first statements from witnesses in a way that influences their testimony.[11] The SFO's Corporate Co-operation Guidance sets out how it assesses co-operation from businesses, [12] including its expectation that companies will consult with the SFO in a timely way before interviewing witnesses.

See Chapter 3 on self-reporting to authorities

Where the authorities are not yet aware of the allegations under review, it is likely that preliminary enquiries will be necessary before the company is in a position to reach a view as to whether to self-report. Where witness interviews are being considered, it may be inappropriate for the authorities to be consulted in advance where a decision to self-report has not yet been made. This can create a tension between the authorities' expectations to be notified as well as the need for the company to bear in mind the risks of prejudicing a future investigation.

Where an investigating authority is already involved, it is prudent for the company to consult or inform it prior to undertaking interviews. Increasingly the SFO and the FCA have sought to impose restrictions on the conduct of interviews in corporate investigations or to prevent them from taking place. While a company cannot be prevented from undertaking its own interviews, there is risk of criticism if it proceeds without the consent of the authority, particularly where it could be suggested that it has prejudiced an investigation. In particular, there may be circumstances where an investigating authority requests that the company refrain from conducting witness interviews during

9 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA, at the 2nd Annual GIR Live, London, 28 April 2016.

10 Speech by Alun Milford, then General Counsel, SFO, at the 14th Annual Corporate Accountability Conference, Congress Centre, London, 9 June 2016 (as reported by Global Investigations Review (GIR) on 10 June 2016).

11 Speech by David Green QC, then Director, SFO, at the GIR Roundtable: corporate internal investigations, 27 July 2015.

12 SFO Operational Handbook, Corporate Co-operation Guidance, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

© Law Business Research 2021

its investigation. Indeed, the judgment handed down by Mr Justice Williams[13] in the DPA reached between SFO and Serco Geografix Ltd referred to the agreement of the company not to interview witnesses during the criminal investigation as an example of its co-operation.[14] The DPA reached with Güralp Systems Limited in 2019 similarly referred to Güralp's decision to defer interviews until the SFO was content for it to proceed, and to provide details of those witness interviews to the SFO as evidence of extensive co-operation.[15]

Providing details of the interviews to the authorities 7.4

In the absence of a statutory duty to co-operate with the authorities with respect to its witness interviews, guidance comes in the form of codes of practice, guidelines, speeches and precedents. Authorities often expect details of witness interviews to be provided, and it is crucial to consider beforehand the purpose of the interview, its intended audience, record-keeping and, if appropriate, to what extent and how this information is to be shared.

The SFO's Corporate Co-operation Guidance sets out its expectations when assessing a company's level of co-operation, which includes preserving available evidence and providing it promptly in an evidentially sound format.[16]

It provides that: 'Organisations seeking credit for co-operation by providing witness accounts should additionally provide any recording, notes and/or transcripts of the interview and identify a witness competent to speak to the contents of each interview.'[17]

The SFO has made clear its expectation that for a deferred prosecution agreement (DPA) to be considered, co-operation must be forthcoming and according to the Code of Practice on Deferred Prosecution Agreements, co-operation encompasses the identification of relevant witnesses, disclosure of their accounts and the documents shown to them and, 'where practicable', ensuring witnesses are available for interview when requested. The SFO's Operational Handbook (in the DPA section) underlines co-operation as a key factor when considering whether to enter into a DPA, and its Corporate Co-operation Guidance states: 'An organisation that does not waive privilege and provide witness accounts does not attain the corresponding factor against prosecution that is found in the DPA code.'

The Director of the SFO, Lisa Osofsky, said in a speech in 2019 that companies needed to take certain steps for their efforts to count as co-operation: 'First, in carrying out their own investigation, we need to see the ultimate

13 *SFO v. Serco Geografix Limited*, Deferred Prosecution Agreement (Case No. U20190413) [2019] 7 WLUK 45.

14 ibid. at para. 24.

15 *SFO v. Güralp Systems Limited*, Deferred Prosecution Agreement, Statement of Facts.

16 SFO Operational Handbook, Corporate Co-operation Guidance at p. 1, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

17 ibid. at p. 5.

© Law Business Research 2021

objective of cooperating with law enforcement by preserving vital evidence such as first-hand accounts and witness testimony."[18]

In *(SFO) R v. Sweett Group PLC* (unreported), Sweett Group's refusal to hand over details of the witness interviews undertaken during its internal investigation was deemed unco-operative by the SFO.

The DPA with Güralp Systems Limited in 2019 referred to the extensive co-operation through provision of information from witness interviews. Co-operation was similarly referred to in the DPA between the SFO and Airbus SE in January 2020 despite the company being slow to engage with the SFO, with the SFO examining internal investigation documents, including interviews, over which Airbus had waived privilege on a limited basis.[19] More recently, the DPA between the SFO and Airline Services Limited (October 2020) also referred to the provision of full co-operation to the SFO.[20]

This contrasts with the DPA between G4S Care and Justice Systems (UK) Limited and SFO (July 2020)[21] where the reduction in financial penalty for assistance to the prosecution and guilty plea was 40 per cent, reflecting the 'delayed nature of G4S C&J's substantial cooperation with the SFO's investigation'. The judgment noted the 'less than full co-operation with the SFO investigation until a relatively late stage'.

While the SFO clearly expects to be told what witnesses have to say in interviews (with a particular emphasis on 'first accounts'),[22] what is less clear is how the detail of the accounts should be imparted and the level of detail that is required. In the case of *SFO v. ICBC SB*,[23] it was sufficient for oral reports of first-account witness evidence to be provided by the bank to the SFO to enable full co-operation to be established.[24]

Summaries of witness interviews were similarly supplied by Rolls-Royce in the context of its DPA reached in January 2017,[25] with, Sir Brian Leveson, then President of the Queen's Bench Division, noting within his judgment the 'extraordinary cooperation', referring to the disclosure of interview memoranda (on a limited waiver basis) as an example of this, and that the company co-operated with the SFO's requests in respect of 'the conduct of the internal investigation, to include the timing of and recording of interviews and reporting

18 Speech by Lisa Osofsky, Director, SFO, at the Royal United Services Institute, 3 April 2019.

19 *SFO v. Airbus SE* (Case No: U20200108).

20 *SFO v. Airline Services Limited* [2020] at para. 52.

21 *SFO v. G4S Care and Justice Services (UK) Limited* (Case No. U20201392).

22 Speech by Alun Milford, then General Counsel, SFO, to an audience of compliance professionals at the European Compliance and Ethics Institute, Prague, 29 March 2016.

23 *Serious Fraud Office v. Standard Bank Plc* (now known as ICBC Standard Bank plc): Deferred Prosecution Agreement (Case No. U20150854).

24 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, at the Managing Risk and Mitigating Litigation Conference 2015, 1 December 2015.

25 *SFO v. Rolls-Royce plc*, Deferred Prosecution Agreement (Case No. U20170036) [2017] Lloyd's Rep FC 249.

© Law Business Research 2021

findings on a rolling basis'.[26] However, in 2017 the former SFO General Counsel refuted suggestions that the provision of summary notes would be standard practice in all cases[27] and that it is not the case that summaries will always be sufficient.[28]

In the case of *SFO v. Sarclad Ltd*,[29] oral summaries were provided without the company's badge of 'genuine co-operation' being compromised. However, the SFO's decision to accept oral proffers in this case was subject to judicial scrutiny in *R (on the application of AL) v. SFO*,[30] with Mr Justice Green describing the provision of summaries as 'highly artificial', questioning the SFO's decision not to take a more robust stance. The SFO was similarly criticised for its failure to challenge the assertion of privilege and require the notes in circumstances where it believed the material not to be privileged.

While the SFO's approach has not always been consistent, it is unlikely that the SFO would accept oral summaries for key witnesses in future to secure a DPA.

The FCA expects regulated firms to notify it of any matters that occur in an internal investigation, in accordance with its Principle 11 obligation.[31] While this does not explicitly apply to witness interviews, the FCA Enforcement Guide makes clear that if the FCA is ultimately asked to rely on submissions or an investigation report in the context of its own decision-making powers, it would ordinarily expect the firm to provide the underlying material, which could include notes of witness interviews, in addition to the report itself.[32] While the level of information will undoubtedly differ from case to case, the FCA has indicated that an oral report may not be sufficient and that information should be shared in a transparent manner, with a proper record.[33] Furthermore, if an individual performing a controlled function or a member of senior management is suspended, a firm must submit a Form C explaining the reasons for suspension.[34]

---

26 ibid. at para. 121.

27 Speech by Alun Milford, then General Counsel, SFO, at GIR London Live, 27 April 2017 (reported by GIR on 27 April 2017).

28 Speech by Alun Milford, then SFO General Counsel, SFO, at the Cambridge Symposium on Economic Crime 2017, Jesus College, Cambridge, 4 September 2017.

29 *SFO v. XYZ Limited*, Deferred Prosecution Agreement (Case No. U20150856). The defendant was subsequently identified in July 2019 as Sarclad Ltd following the acquittals of three Sarclad employees.

30 *R (on the application of AL) v. Serious Fraud Office* [2018] EWHC 85.

31 For dual-regulated firms, the Prudential Regulation Authority's [PRA] Fundamental Rule 7 obligation will also apply: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/new-bank/Fundamentalruleprinciples.

32 FCA Enforcement Guide, para. 3.11.10.

33 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA, at the Pinsent Masons Regulatory Conference 2015, 5 November 2015.

34 SUP 10.13 Changes to an approved person's details.

© Law Business Research 2021

The guidance surrounding co-operation with the authorities and what is expected continues to evolve. In cases where the company or its employees are at risk of further investigation, prosecution or civil action, the company will want to consider the benefits that early co-operation may bring. However, whether it is in the interests of the company to co-operate will depend on the facts of each case.

7.5 Identifying witnesses and the order of interviews

Where interviews are to be conducted, the company, its representatives, or both, should seek to interview all company personnel who were involved in the facts under investigation, including those who should have been involved by virtue of their position. Reporting lines of those involved should also be considered. The witness list may expand as more information becomes known, and should therefore be reviewed regularly.

Employees generally have a duty to co-operate and are likely to owe a duty of candour towards their employer, and a failure to comply could result in disciplinary action.

See Chapter 19 on whistleblowers

If there is one, it may be preferable to interview a whistleblower at the start of the process. The structure of an investigation is fact-specific, but, broadly, the order of other interviews should be based on the level of risk that the witness poses to the business, beginning with those who present the least risk. For the most part this is likely to follow levels of seniority, starting with lower-level employees and leaving senior management until later. Timing considerations sometimes mean witness interviews need to be taken out of the normal order, and consideration should be given to the creation of a 'leavers list' to ensure that potential witnesses who are due to leave the company are identified.

See Section 7.6

The benefit of this approach is that the company may be better positioned to obtain an overall sense of the extent of the issues before focusing on particular areas of risk, although it is important that sensitive or confidential information is not referred to unless strictly necessary as there is risk that information may be shared.

While it may be appropriate to conduct early interviews with senior employees to obtain initial accounts (particularly where there is likely to be more than one opportunity to interview), generally members of senior management should be interviewed when the investigation is further advanced. Typically, senior employees are more likely to pose a greater risk from the perspective of corporate liability and therefore it is important that any potential risks are identified beforehand. Under the principle of identification, in the United Kingdom, a company can be criminally responsible for the actions of those employees that represent the 'directing mind and will' of that company,[35] generally restricted to board directors, the managing director and other senior

35 *Lennards Carrying Co and Asiatic Petroleum* [1915] AC 705, *Bolton Engineering Co v. Graham* [1957] 1 QB 159 (*per* Denning LJ) and *R v. Andrews Weatherfoil* 56 Cr App R 31 CA.

© Law Business Research 2021

officers who carry out management functions on the company's behalf.[36] The principle of identification is explored in more detail in Chapter 1.

This can cause difficulties when interviewing board members and senior management who may be the 'client' for the purposes of the investigation but who may need to be interviewed in the context of their own involvement. For the most part this can be avoided by identifying the 'client' at the outset of the case as made up of a group of senior employees or board members with no involvement in matters under investigation. However, depending on the size of the company and the nature of the case, this is sometimes unavoidable and therefore the basis on which the interview is being conducted must be made clear to the witness.

See Chapter 5 on beginning an internal investigation

There are a number of statutory exceptions to the principle of identification, such as the offence of failure to prevent bribery, and the government has been examining the case for reform of the law on corporate liability for economic crime.[37] The Law Commission has been tasked by the Ministry of Justice to undertake a review of the law relating to the criminal liability of non-natural persons, including companies, and has been asked to provide options for reform. At the time of writing, the Law Commission is consulting on its review, and is expected to present an options paper in early 2022.[38]

When the issues under investigation fall within the statutory exceptions,[39] it can be difficult to identify the appropriate individual to interview on behalf of the company. Again, the purpose of the interview and the basis on which it is being conducted needs to be made clear from the outset.

Senior employees are also more likely to owe fiduciary duties to the company and potentially be liable for breaches of those duties and become defendants in civil proceedings by the company. As a result, these interviews should generally take place when the company is in a better position to identify the extent of any breaches.

See Chapter 5 on beginning an internal investigation

Relevant information may also be sourced through interviews with third parties including former employees, customers and contractors. The obvious benefit is that these witnesses may be more forthcoming where there is no risk of disciplinary proceedings. However, third parties cannot generally be required to attend an interview, and unless there is a contractual obligation requiring their attendance, they may refuse to attend. Even in circumstances where a contractual obligation exists this could be difficult to enforce, as could a confidentiality clause. The interview process itself is also likely to notify the third party of the investigation and the subject matter under review and

36 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153 and *SFO v. Barclays* [2018] EWHC 3055 (QB).

37 Call for evidence: Corporate and Economic Crime – 13 January 2017 to 31 March 2017.

38 https://www.lawcom.gov.uk/project/corporate-criminal-liability/.

39 Bribery Act 2011, s.7; Criminal Finances Act, ss.45 and 46; Corporate Manslaughter and Corporate Homicide Act 2007, s.1.

© Law Business Research 2021

depending on the nature of the relationship, it may not be appropriate to interview him or her at that time, particularly when the decision on self-reporting is outstanding.

7.6 When to interview

See Section 7.11 and Chapter 36 on privilege

The timing of interviews can be influenced by a number of factors, including the stage of the investigation and whether or not any record of interview would be covered by legal privilege. Scoping interviews usually take place at the outset of an investigation, most likely with a few individuals who have a general knowledge of the subject matter under investigation.

Substantive interviews are likely to be most effective once the bulk of any document review has taken place. This will allow for any key documents to be identified and put to the witness, and for questions to focus on the areas of risk. It is best to plan for only one interview; while there may be circumstances where a second or third interview is appropriate, it is by no means guaranteed that the witness would agree.

Timing of the interviews can pose particular difficulties when there are competing considerations. For example, it may be necessary to delay when the company has a claim for injunctive relief against individuals, to avoid assets being dissipated in advance of a freezing order being granted. However, it could be that there is only a limited amount of time to interview an employee who is leaving the company or the company may need to speak to an individual at short notice to assist in an assessment of whether to self-report. Clearly such factors need to be prioritised.

It is important to allow flexibility for factors outside the company's control. . Where the corporate investigation is likely to remain an internal review, there is little risk to the company conducting interviews to a timetable that suits it, although the company will wish to consider whether legal privilege would apply. Where there is suspicion of a criminal or regulatory violation and a formal investigation has commenced, there are a number of risks associated with conducting interviews in parallel with these investigations.

See Section 7.11 and Chapter 36 on privilege

As a general point, any interviews with individuals at risk of criminal exposure should be postponed until all evidence has been secured, to minimise the risk of evidence being destroyed. This is particularly important where a criminal or regulatory investigation is likely. Similar concerns apply where the individuals are potential defendants to civil proceedings by the company.

Both the SFO and the FCA place significant emphasis on the first accounts of witnesses, and take the view that they can help inform an understanding of what went on and allow for the accuracy or integrity of a witness to be tested. However, depending on the facts of the case, this view can often be misplaced; the first account given by a witness is not necessarily always the best one, particularly in complex investigations that span a number of years and where there is extensive underlying material. The quality of a witness's evidence can often be improved having been given the opportunity to review the evidence and recall the context. Nonetheless, the SFO and FCA have

© Law Business Research 2021

increasingly sought to place restrictions on interviews of key suspects in corporate investigations and may seek to prevent them altogether.

In such circumstances it may be prudent for a company to seek to agree an approach with the authorities prior to conducting any interviews.

The authorities are also increasingly sensitive to the risks of witness contamination, and a company whose conduct of witness interviews has caused prejudice to a criminal or regulatory investigation could be subject to serious criticism. At best this could involve comment or views that are unhelpful for the company; at worst this could include allegations of perverting the course of justice. Mark Steward, Director of Enforcement and Oversight at the FCA has commented on the importance of an 'independent public body investigation' being able to conduct itself without 'the crime scene being trampled over'.[40] The SFO has similarly made clear that corporate investigations that 'trample over the crime scene' are unhelpful and that integrity of evidence, especially regarding witness accounts, should be respected,[41] and has noted that internal investigations may result in first accounts of witnesses being taken, delivered or recorded in a form which may be less than full and accurate, as opposed to recording the account by way of a transcript.[42] The SFO's former Joint Head of Bribery and Corruption, during a speech in 2018, commented: 'The data needs to be identified, collected, preserved and analysed in a way that does not tip off potential suspects into deleting data and protects its integrity and continuity.'[43] The SFO's Corporate Co-operation Guidance lists indicators of good practice including consulting with the SFO in a timely way before interviewing potential witnesses or suspects, and refraining from tainting a potential witnesses' recollection, for example by sharing or inviting comment on another person's account or showing the witnesses documents that they have not previously seen.

When a criminal or regulatory investigation is anticipated or already under way, a company may wish to consider engaging with the authorities at an early stage to avoid any criticism that might follow. However, engaging with the authorities may not necessarily be appropriate in every case and runs the risk of loss of control. Each case will need to be assessed on its specific facts and surrounding circumstances, and interviews should always be conducted so as to minimise the risk of contamination or prejudice.

40 Speech by Mark Steward, Director of Enforcement and Oversight, FCA, at the 14th Annual Corporate Accountability Conference, Congress Centre, London, 9 June 2016 (as reported by GIR on 10 June 2016).

41 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, at the Global Anti-Corruption and Compliance in Mining Conference 2015 on 20 May 2015.

42 Speech by David Green QC, then Director, SFO, at the GIR Roundtable, 27 July 2015.

43 Speech by Camilla de Silva, then Joint Head of Bribery and Corruption, SFO, at the ABC Minds Financial Services conference, 15 March 2018.

© Law Business Research 2021

7.7 Planning for an interview

Interviews in a corporate investigation can be conducted by various people: internal or external lawyers, accountants, forensic experts, specialist investigators, HR or compliance officers, and others. Careful thought should be given to who is best placed to undertake them.

As a general rule, where a company is engaged in a corporate investigation into allegations of criminal or regulatory misconduct, it is preferable to have lawyers (internal, external or both) present at interviews to take notes and identify the key risk areas, to enable confidentiality and for any claim to privilege to be strengthened. Generally, it is preferable for the same person or persons to conduct the interviews of all those witnesses who provide similar types of information to allow for consistency of approach and for the credibility of witnesses to be more readily assessed. It is also preferable to have two interviewers present to allow for one to take notes while the other asks questions.

Where external lawyers have been instructed, they should generally conduct the interviews. External lawyers often bring (and importantly are seen to bring) expertise, objectivity and independence, which can be very important when assessing the credibility of the investigation. Although it can bring a degree of formality that can make the experience more daunting for the witness, the use of external lawyers will strengthen a claim to legal privilege.

Where external lawyers have not been instructed, the company may consider resourcing the process internally by using compliance personnel, internal auditors or HR officers, or by using in-house lawyers. Either way, those conducting the interview should not have had any involvement in the allegations under review. While the use of non-lawyers may decrease the levels of concern among employees, in general they may be less skilled in conducting these types of interviews and less familiar with the issues that may arise. In-house lawyers will have a good understanding of the business and legal advice given to the company will generally be privileged in the United Kingdom. However, the protection of legal privilege will not apply to advice given by in-house lawyers in the context of European Commission related investigations,[44] and it may be necessary in those circumstances to engage external lawyers.

See Section 7.11 and Chapter 36 on privilege

Where forensic experts (internal or external) are engaged it may be prudent to involve them in interviews with key individuals. If so, it is generally advisable for these interviews to be conducted alongside internal or external lawyers to ensure that the contents can be covered by the company's confidentiality and privilege, as appropriate, and to strengthen a claim to this privilege.

Prior to the interview, a core bundle of documents relevant to the particular witness should be prepared. Consideration should be given to whether the witness is given access to documents, either before or during an interview, and what documents, if any, should be put to the witness. Referring to documents

44 *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission*, Case C-550/07 P.

© Law Business Research 2021

can be a very useful tool to assist in refreshing a witness's memory and to allow for specific comment. Key documents can be put to provide a better understanding of their content and to give an opportunity for the witness to provide an explanation.

In general, copies of confidential or sensitive documents should not be given to witnesses where there is a risk these could be shared or used contrary to the company's interests. In complex matters, providing pre-interview disclosure will enable the witness to prepare; however, in general this should be done on a restricted and confidential basis with the requirement that they are either returned or destroyed at the conclusion of the interview. It is preferable that a witness is not given documents that he or she has not previously seen. Where the interview is to be conducted remotely, access could be given to material on a secure data sharing platform or screens could be shared, and the need for confidentiality and security of data remains.

See Chapters 5 and 6 on beginning an internal investigation; and 11 on production of information to authorities

The provision of documents may give rise to data protection issues in light of the company's obligations under the data protection principles,[45] and particularly where multiple jurisdictions are involved.

A detailed interview plan can be useful to ensure that all relevant questions are put to the witness, although this should not be restrictive, and in general, topics should be addressed in a chronological order that develops facts in a logical way.

When providing topics in advance of an interview, it is generally helpful to indicate the main areas that may be covered to assist the witness to prepare, particularly where the subject matter is complex. However, giving a list of detailed questions is generally not appropriate, as questions are likely to evolve as the interview progresses, and there is also a risk that the questions might be shared.

Interviewers should ask questions in a measured and courteous manner with a clear and professional tone. There is little point in adopting an aggressive approach or engaging in lengthy cross-examination; this is unlikely to be effective and could give rise to criticism, or employment or personal injury claims. A skilled interviewer will seek to put the witness at ease before addressing the key topics. Where there are two interviewers, different interviewing styles can often be effective.

Conducting the interview: formalities and separate counsel 7.8

Professional obligations can affect how witness interviews are conducted. Solicitors have a duty to act in their client's best interests,[46] and they must not take unfair advantage of a third party.[47] These duties do not always align and it is therefore important to balance the competing requirements.

45 UK General Data Protection Regulation, Article 5.

46 SRA Principle 7.

47 SRA Code of Conduct for Solicitors, Chapter 1.2.

© Law Business Research 2021

The interviewer should be satisfied that the witness understands the basis on which is they are being interviewed, the purpose of the interview and the use that could be made of the information provided. This may impact its admissibility.

In the United States, an *Upjohn* warning is given at the start of the interview, where lawyers are present. This practice is often adopted in many investigations in the United Kingdom, even where there is no involvement of US authorities at that time. The warning sets out that:

- the lawyers represent the company and not the employee or witness;
- privilege in the interview belongs to the company and not the employee; and
- the company might choose to waive its privilege and disclose matters discussed in interview to the authorities.

Upjohn warnings derive from the case of *Upjohn Co v. United States*,[48] where it was held that the privilege that attaches to communications between a company's lawyers and its employees is the company's privilege, and not that of its employees. While there is no formal requirement for these warnings to be given in the United Kingdom, it is considered best practice to do so.

The witness should be reminded of the confidential nature of the interview and, where appropriate, be told that it is a fact-finding exercise. If a company has decided to waive privilege prior to the interview and provide details to the authorities, the *Upjohn* warning may need to be strengthened. The company could consider whether to give a more formal caution, similar to that given by the police when investigating suspects, although this will rarely be required. If necessary, the witness should be told that while not part of a disciplinary process, the information provided could inform a decision on whether to instigate disciplinary action.

The company should consider whether its own legal advisers can advise the witnesses or whether to allow them to have their own lawyer in attendance. The company may wish to offer to pay for the independent legal adviser. Clearly a company cannot prevent its employees obtaining legal advice of their own volition and expense; however, it can control who can be present in an internal interview. If an authority investigation is under way, the witness may have contractual rights or rights under an insurance policy (D&O insurance) to fund an independent legal adviser. Former employees may have an indemnification or contractual right as part of their exit package.

Those witnesses who appear to be at little risk of criminal or regulatory exposure are unlikely to need independent counsel to protect them against any risk of self-incrimination, and the provision of an *Upjohn* warning or a similarly worded preamble should suffice. However, a company may nonetheless offer separate legal advice to these witnesses if this would allay their concerns or ensure that appropriate advice is given (including from an employment or civil

48 *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

© Law Business Research 2021

perspective). Perhaps most importantly, an independent adviser's role will assist preparation and increase the likelihood that the individual will give their best account. Moreover, it is often not easy to predict where risks may be at an early stage. Where the interview is conducted remotely and the witness is advised by an independent legal adviser, thought should be given to allowing a separate remote consultation room which can allow confidential and privileged access to that legal advice.

The provision of independent legal advice is particularly important where there may be a conflict of interest between the company and a witness. This can arise where a witness is a whistleblower or at risk of criminal or regulatory investigation, or where the company could be implicated in corporate wrongdoing. In these circumstances the interests of the company and the witness may not align and it would be prudent to consider suggesting an independent legal adviser While the interview may be delayed to allow advice to be given, it ensures that the witness has had the opportunity to obtain their own legal advice and, depending on the facts, could make the interview more effective. Conversely, the involvement of an independent legal adviser could result in the witness being less inclined to attend the interview or answer questions, although an employee would then be at risk of disciplinary action for not co-operating.

The decision when to offer independent legal advice may also depend on the account given by the witnesses, and it may be appropriate to stop interviews if they give an account that indicates that the company has a potential civil claim against them or that they are making potential criminal admissions.

Ultimately it would be difficult for witnesses to assert that they had not been fully informed where they had been separately represented, or that the interviewer or company had taken an unfair advantage.

Conducting the interview: whether to caution the witness 7.9

Where a witness may be suspected of involvement in a criminal offence, a caution may be considered. A caution is used by police officers and other investigators when conducting interviews of suspects to ensure that any resulting account (or refusal to answer questions) is admissible in criminal proceedings.[49]

The duty to caution applies to SFO investigators,[50] but is not restricted to state authorities and can also apply to private store detectives[51] and commercial investigators who are appointed by a company to investigate its employees for the commission of criminal offences.[52] The requirement to caution is, however,

49 Code C, 10.1 PACE Code of Practice for the detention, treatment and questioning of persons by Police Officers and PACE 1984, s.67(9), which provides 'that persons other than police officers who are charged with the duty of investigating offences' shall have regard to the relevant provisions of the PACE Codes of Practice and Code C, 10.1 of the Codes sets out the requirement to caution.

50 *R v. Director of the Serious Fraud Office, ex p Saunders* [1988] Crim LR 837.

51 *Bayliss* (1993) 98 Cr App R 235.

52 *Twaites and Brown* (1990) 92 Cr App R 106.

© Law Business Research 2021

unlikely to arise in an internal investigation where criminal offences are being considered, as the authorities have shown great reluctance to allow a company to interview the suspect and effectively act on their behalf in gathering a suspect's account with a view to it being used at a criminal trial.

Importantly, the duty to have regard to the relevant provisions of the Police and Criminal Evidence Act 1984 (PACE) also does not apply in the context of an internal investigation where the sole purpose is to determine what recommendations should be made to an internal disciplinary panel.[53] It is therefore unlikely to apply in circumstances where an employer investigates allegations that could give rise to disciplinary action and where the sole purpose of the investigation was to inform the company how to respond.

7.10 Conducting the interview: record-keeping

A record can be kept of a witness interview may be kept in a number of ways. Where it is audio-recorded and transcribed a verbatim record would exist, removing the risk of any challenge to the accuracy of what was said, and the recording would capture the tone and any pause or emphasis, which can often give context and allow for an overall assessment. However, it could affect the witness's account by adding an element of formality, potentially having an unsettling effect on the interviewee who might become less forthcoming. More importantly, there is significant uncertainty over whether legal privilege would apply to a recording, particularly where the interview has been conducted as a fact-finding exercise. Even where privilege can be properly asserted, it is likely to be challenged by the authorities, and where a transcript exists, the authorities are likely to request a copy.

See Section 7.11 and Chapter 36 on privilege

An alternative approach is for the legal adviser to prepare a note of what the witness has said. Legal privilege is more likely to apply in circumstances where notes contain some form of legal comment, advice and analysis. This may include the lawyer's own impressions and assessment of the interview. Alternatively, two sets of notes could be prepared, one containing the factual account and one containing the lawyer's own views. If so, at a minimum, the authorities are likely to seek a copy of the factual account.

The company will need to decide whether to provide the witness with a copy of the note. Where it is likely to rely on the witness's testimony in civil proceedings, it may be helpful to agree a note at an early stage to limit any future challenge to its accuracy. This, though, carries the risk that it may be passed on and any applicable privilege would be lost, and may cause issues if the account is materially disputed.

Where proceedings are anticipated, there are some advantages in preparing a witness statement at an early stage. If the witness decides at a later date not to co-operate or for whatever reason he or she is no longer able to assist, the company may be able to rely on the evidence given, or compel the witness to

53 *R v. Welcher* [2007] EWCA Crim 480.

© Law Business Research 2021

attend and give evidence having already taken a record of the witness's evidence. However, even if privilege can be maintained, it is likely the authorities would nevertheless seek a copy.

Where interviews are conducted remotely, steps should be taken to ensure that the interview remains confidential and to limit the risks of it being recorded either deliberately or inadvertently.

Legal privilege in witness interviews 7.11

Legal privilege in witness interviews raises a number of complex issues, and a claim to privilege will be closely scrutinised by the authorities. Over the past few years, the SFO has claimed that it does not want to undermine legal privilege, which is respected as a legal principle and fundamental right, but that any decision to waive privilege would be viewed as a positive feature.[54] The SFO has said it is not interested in material that is 'genuinely privileged', but that it will challenge 'overly ambitious' privilege claims, and that a company's decision to structure its investigation so as not to attract privilege would be viewed as significant co-operation.[55]

During a speech in April 2019, Lisa Osofsky commented that legal professional privilege is recognised as a 'fundamental right in our legal system', but that companies can waive that privilege if they wish to cooperate with the Serious Fraud Office. This was a precursor to the Co-operation Guidance that followed.

When an organisation elects not to waive privilege, the SFO nonetheless has obligations to prospective individual defendants regarding disclosable materials.

The existence of a valid privilege claim must be properly established; the company will be expected to provide certification by independent counsel that the material in question is privileged. If privilege is not waived and a trial proceeds, where appropriate the SFO will apply for a witness summons under section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965.

An organisation that does not waive privilege and provide witness accounts does not attain the corresponding factor against prosecution that is found in the DPA Code, but will not be penalised by the SFO.

If a company chooses not to co-operate with the SFO, it is unlikely to be offered a DPA.

Companies should note the risk that disclosing information relating to witness interviews could result in a waiver of privilege more generally. Ultimately the information could be shared with authorities in other jurisdictions or be disclosable in criminal proceedings against third parties (e.g., former

54 Speech by Hannah von Dadelszen, then Joint Head of Fraud, SFO, at the Pinsent Masons Business Crime and Compliance conference, London, 9 November 2018.

55 Speech by Camilla de Silva, then Joint Head of Bribery and Corruption, SFO at the Herbert Smith Freehills Corporate Crime Conference 2018, 21 June 2018.

© Law Business Research 2021

employees) which might follow from the company self-reporting, or in other proceedings that may not be in the company's best interests. While this risk may in part be mitigated by a limited waiver agreement, this would not necessarily extend to other jurisdictions and is unlikely to prevent the SFO from disclosing documents in criminal proceedings if statutory obligations require it to do so. Once disclosed or shared with authorities in other jurisdictions, confidentiality may in due course be lost, for example if a defendant relies on a privileged document at trial. The Law Society of England and Wales provides guidance to lawyers about their duty to act in the best interests of clients, including maintaining their claim to privilege.

The law surrounding legal privilege and records of interviews is complex and evolving. It has been made more complicated by the narrow interpretation of privilege that has been taken in several recent court decisions. These cases are summarised below.

See Chapter 36 on privilege

It was held in *The RBS Rights Issue Litigation*[56] that the interview notes prepared by the bank's legal representatives were not subject to legal advice privilege (it was accepted that litigation privilege did not apply). The court found that, for the purposes of legal advice privilege, the 'client' consists only of those employees authorised to seek and receive legal advice from the lawyer. In relation to interviews with witnesses, it found that privilege does not extend to information provided by employees and ex-employees outside the client group, and that in order for the lawyers' working notes of the interviews to attract legal advice privilege, they must contain 'some attribute or addition such as to betray or at least give a clue as to the trend of advice being given to the client by its lawyer',[57] which the bank had failed to demonstrate.

This judgment was followed by the High Court in *Director of the SFO v. ENRC*.[58] ENRC's argument that legal advice privilege applied to lawyers' notes of interviews was rejected at first instance, and Mrs Justice Andrews found that the question of whether legal advice privilege applied was an evidential one as to whether the notes demonstrated the legal analysis and 'tenor' of the advice.[59] The judgment referred to examples of the type of evidence required to attract legal advice privilege, including a qualitative assessment of the evidence or any thoughts about its importance or relevance to the inquiry or indications of further areas of investigation that the author of the notes considered might be fruitful, and noted that the betrayal of further lines of investigation would not in itself have been sufficient to render the notes privileged.[60]

56 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

57 ibid. at para. 107.

58 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205.

59 ibid. at para. 97.

60 ibid. at para. 180.

© Law Business Research 2021

Applying the case of *Three Rivers (No. 5)*,[61] Andrews J held that legal advice privilege would only apply to communications between the lawyer and those authorised by the company to obtain legal advice on its behalf, and therefore not to employees or former employees more widely.[62]

Andrews J's decision was appealed, and although the Court of Appeal did not need to reach a decision on issues relating to legal advice privilege (because of its decision on litigation privilege), it nevertheless gave its view (*obiter*) on how it would have decided those issues. The Court would have found that *Three Rivers (No. 5)* had been correctly interpreted by Andrews J (and by courts on other occasions) as having created a general rule that, in a corporate context, only the communications of those employees authorised by the company to seek and receive legal advice on its behalf are capable of attracting legal advice privilege.[63] Significantly however, the Court gave a strong indication that it felt *Three Rivers (No. 5)* had been wrongly decided and would have been in favour of departing from that case had it been open to it to do so, although ultimately it felt this is a question that only the Supreme Court can determine.[64]

ENRC's claim for litigation privilege was also rejected by Andrews J at first instance, who was not satisfied that, on the facts, litigation was in reasonable contemplation at the pertinent times or that, in any event, the dominant purpose of the documents coming into existence was for use in the conduct of litigation. It was held that an SFO investigation was seen as a preliminary step and that a prosecution only becomes a real prospect once evidence is discovered to substantiate the allegation, or where the accusations appear to be true.[65]

The Court of Appeal disagreed with Andrews J's conclusion of the facts, holding that at the time the documents came into existence, ENRC reasonably contemplated a prosecution by the SFO.[66] While the Court did not necessarily disagree with Andrews J's view that an SFO investigation in itself could not constitute adversarial litigation for the purposes of litigation privilege, it ruled that in circumstances where the SFO 'makes clear to the company the prospect of its criminal prosecution' and legal advisers are engaged to deal with this, 'there is a clear ground for contending prosecution is in reasonable contemplation'.[67]

Although the Court did not accept ENRC's alternative argument that once an SFO investigation is in reasonable contemplation so too is a prosecution, it held that in this case the evidence 'pointed clearly towards the contemplation of a prosecution if the self-reporting process did not succeed in averting

61 *Three Rivers District Council v. Governor and Company of the Bank of England (No. 5)* [2003] EWCA Civ 474.

62 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at para. 180.

63 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at paras. 123 and 133.

64 ibid. at para. 130.

65 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at paras. 150 to 163.

66 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 93.

67 ibid. at para. 96.

© Law Business Research 2021

it',[68] and did not feel that the uncertainty a company inevitably experiences when faced with whistleblower allegations is a bar to litigation privilege.[69] Andrews J's suggestion that litigation privilege cannot apply until a defendant either knows the full details of what is likely to be unearthed or a decision to prosecute has been taken.[70]

As to whether the dominant purpose of the documents coming into existence was for conduct of the litigation, the Court of Appeal was satisfied that this requirement was met in this case, and that just because solicitors prepare a document with the ultimate intention of showing it to the opposing party, that does not automatically deprive the preparatory legal work they have undertaken of litigation privilege.[71] Of particular importance was the Court's view that documents prepared for the dominant purpose of avoiding or settling litigation are just as much covered by litigation privilege as those prepared for defending it.[72]

ENRC provides very helpful guidance and several principles of wider application to assist corporates who find themselves in similar situations. However, it also highlights the extent to which questions of litigation privilege in the context of internal investigations turn on the facts (as indeed is the case with all questions of privilege).

In *Bilta & Ors v. RBS & Anor*,[73] the High Court's Chancery Division was concerned with the status of documents created during an internal investigation carried out by RBS's solicitors, relating to a tax dispute with Her Majesty's Revenue and Customs (HMRC). This included transcripts of interviews with employees and ex-employees that had come into existence following a letter from HMRC. Bilta and various other claimants sought disclosure of these documents, which was resisted by RBS on the basis that they were subject to litigation privilege. The Court held that the documents were indeed protected by litigation privilege, with the sending of HMRC's letter considered significant and found to have marked a 'watershed moment', likened to a letter before claim. While RBS may also have hoped to dissuade HMRC from proceeding, it was found that this was only a subsidiary purpose subsumed into the dominant purpose.

In *R (for and on behalf of the Health and Safety Executive) v. Paul Jukes*,[74] following a fatality at work, solicitors instructed by the employer concerned carried out an investigation. A statement was obtained from the appellant Mr Jukes, a former manager, as part of the internal investigation, after the Health and Safety Executive (HSE) had begun its investigation but before

68 ibid. at para. 97.

69 ibid. at para. 98.

70 ibid. at para. 100.

71 ibid. at paras. 102 and 112.

72 ibid. at paras. 102, 113, 118.

73 *Bilta & Ors v. RBS & Anor* [2017] EWHC 3535 (Ch).

74 *R (for and on behalf of the Health and Safety Executive) v. Paul Jukes*, [2018] EWCA Crim 176.

© Law Business Research 2021

it commenced proceedings. This statement was relied on heavily during the subsequent prosecution of the appellant, and following his conviction he appealed, partly on the basis that the trial judge had been wrong to allow the prosecution to rely on the statement as it was protected by privilege. The Court of Appeal rejected this argument and found that at the time the statement was made there was no evidence that anybody within the company knew what the company's and the HSE's investigations would unearth, such that it could be said that prosecution by the HSE was reasonably in contemplation. It was held that the statement was not therefore protected by litigation privilege.

In *Jukes*, the Court of Appeal approved part of the first instance *ENRC* decision. The Court of Appeal in *ENRC* addressed this potential issue but felt that its conclusions were not invalidated by *Jukes*, on the basis that the endorsement of Andrews J's judgment in that case had been *obiter*.

Notes of interviews and the status of privilege were further considered by the High Court in *R (on the application of AL) v. SFO*.[75] A judicial review was brought against the SFO for failing to pursue Sarclad Ltd (initially anonymised as XYZ Ltd) for non-compliance with its DPA through not disclosing the full interview notes, having instead accepted oral proffers.[76] The SFO's position was that there was no need to obtain the interview notes because the company's claims of privilege were 'not obviously wrong'[77] and that it had exercised legitimate prosecutorial discretion in accepting the oral proffers. In the judgment, the SFO was criticised for (among other things) its failure to challenge the assertion of privilege and require the notes in circumstances where it believed the material not to be privileged. It was found that, even if the assertion of privilege could be made out (which, in light of recent case law, the court said was not supported), by providing oral summaries the privilege had been waived. The judgment noted the SFO's failure to fully consider whether to require Sarclad to waive privilege over the notes, given its contractual duty to co-operate under the DPA,[78] and whether privilege had been waived, even on a limited basis.

In the absence of any further judicial interpretation, those conducting internal investigations should therefore be conscious that a claim to privilege of records of interviews with those outside the client group could be subject to challenge, notwithstanding the helpful decision of the Court of Appeal in ENRC, and whether a claim to privilege will be successful will depend on the facts of each case. Where the records could be said to form part of the lawyer's working papers in the context of advice, a claim to legal advice privilege would be strengthened if the notes contained sufficient legal analysis, assessment as to relevance and the 'tenor' of the legal advice. Legal advice privilege will also attach to material that forms part of the continuum of the lawyer–client

75 *R (on the application of AL) v. SFO* [2018] EWHC 856 (Admin).

76 *SFO v. XYZ Ltd* (Case No. U20150856). The defendant was subsequently identified in July 2019 as Sarclad Ltd following the acquittals of three Sarclad employees.

77 *R (on the application of AL) v. SFO* [2018] EWHC 856 (Admin) at para. 7.

78 ibid. at para. 26.

© Law Business Research 2021

communications even where those documents do not expressly seek or convey legal advice.[79] For litigation privilege to apply, litigation must be in reasonable contemplation, and the dominant purpose of the interviews must be the conduct of that litigation. This will depend on the facts of the case, but where litigation is in contemplation, this should be documented to assist in defending any challenge to a claim for privilege.

See Chapter 36 on privilege

Factors that may strengthen a claim to privilege over interview notes include where, for example, notes arise from interviews with likely potential defence witnesses in contemplated litigation or where interviews are conducted with a view to assessing the potential risk the witness may pose in likely proceedings.

Those conducting investigations may wish to consider the timing of witness interviews in the context of when the likelihood of litigation (civil or criminal) is clearer, in the absence of which there is a risk that claims to privilege of records of witness interviews will be challenged.

Where privilege can be established, the best position may be to ensure that any notes taken during interviews are done so as to strengthen a claim to privilege and to leave any decision on whether to waive privilege until the course of the investigation and interests of the authorities are clearer.

7.12 Conducting the interview: employee amnesty and self-incrimination

As a general point, an employer cannot provide amnesty from criminal or regulatory action. Similarly, an agreement cannot prevent disclosures to regulators or inhibit criminal investigations.

While in theory amnesty against internal disciplinary action could be offered, this is very rare. More commonly, discussions take place with a view to the employee leaving under the terms of a settlement agreement, which can include a financial settlement and avoids the employee being dismissed. Such discussions can take place 'without prejudice', or they may take place as 'protected conversations' and therefore should not take place during a witness interview. These discussions, providing they meet the required criteria, cannot be used as evidence in unfair dismissal proceedings,[80] although, unless the without prejudice rule can genuinely apply, they could be used in whistleblowing or discrimination claims.

See Chapter 13 on employee rights

Though in theory it is possible for an employer to agree a certain course of action (for example, to retain an employee and waive the right to bring disciplinary action), this would not be advisable in circumstances where facts are not yet known or understood. If an amnesty is given, the employer would want to ensure that any waiver against disciplinary action related to closely defined and identifiable incidents only.

Employers also need to be wary of consistency. Where two employees have committed misconduct, allowing one employee to remain and dismissing

79 *Balabel v. Air India* [1988] 1 Ch 317.

80 Employment Rights Act 1996, s.111A.

© Law Business Research 2021

another would support an unfair dismissal claim that the dismissed employee may bring. The employer would need to justify the difference in treatment, which may be easier to do when an employee has left under the terms of a settlement agreement.

An employee may also seek to claim privilege against self-incrimination and refuse to answer questions on that basis, particularly where he or she is advised by an independent legal adviser. While there may be clear advantages to this approach from a criminal or regulatory perspective, this in itself would not provide a defence against dismissal. An employer could reach a decision to dismiss on the basis of the information that it had at that time. Though it cannot compel employees to answer questions, their failure to do so could be deemed to be unco-operative and in breach of the terms and conditions of employment, resulting in further grounds for disciplinary action. A dismissal for gross misconduct can still be fair in circumstances where a decision has been made not to prosecute, or where the employee has been acquitted of criminal charges for the same offence.[81] Acts that could constitute gross misconduct are broader than criminal offences and the requirement that gross misconduct be 'fair' is lower than the criminal standard of proof.[82]

In addition to employment considerations, it is always possible for an employer to agree not to pursue civil claims against an employee in return for information being provided. However, as set out above, this should generally not be offered until the full facts have been established.

Considerations when interviewing former employees 7.13

In general, unless there is a contractual commitment to do so, former employees can simply refuse to attend a witness interview. It is important to bear this in mind when negotiating an employee's exit, although in reality (depending on the specific contract terms), once the employee has left there may be little a former employer can do to require attendance, even if it enjoys the benefit of a contractual commitment from the employee to co-operate in any future investigation or proceedings. Former employees regulated by the FCA have a duty under Statements of Principle and Code of Practice for Approved Persons (APER) Principle 4 to co-operate with the regulators.[83] It is unlikely that this

81 *Okhiria v. Royal Mail* UKEAT/0054/14/LA.

82 A dismissal for gross misconduct is 'fair' if the employer believed that the employee was guilty of gross misconduct, if it had reasonable grounds on which to base that belief, and if it had carried out as much investigation as was reasonable in the circumstances of the particular case: *British Home Stores Ltd v. Burchell* [1978] UKEAT 108_78_2007. In a criminal trial, the standard of proof required is to prove guilt 'beyond a reasonable doubt'.

83 The Statement of Principle 4 (see APER 2.1A.3 R) is in the following terms: 'An approved person must deal with the FCA, the PRA and other regulators in an open and cooperative way and must disclose appropriately any information of which the FCA or the PRA would reasonably expect notice.'

© Law Business Research 2021

provision would require them to assist with an internal investigation, and if asked, they could fairly argue that their duty was to the regulator.

Where a former employee is interviewed there are some protections available in respect of whistleblowing, discrimination or victimisation, should they arise in the conduct of the interview or how he or she is treated afterwards. An employer should be wary of giving assurances of anonymity to a former employee in respect of information given, although this could be given on a need-to-know basis. Anonymity should not be guaranteed where regulatory obligations exist or where it could inhibit any criminal investigation, and assurances that any statement provided would not be disclosed to criminal or regulatory authorities should not be given.

See Chapters 5 on beginning an internal investigation; and 11 on production of information to authorities

Data protection issues may also arise if the account or statement given by a former employee contains personal data. Care also should be taken in global investigations that data protection rules from relevant jurisdictions are considered.

See Chapter 40 on data protection

7.14 Considerations when interviewing employees abroad

Interviewing witnesses abroad can present particular challenges. Statutory employment law is generally of geographical rather than universal jurisdiction and, as a result, statutory employment laws of the jurisdiction where an employee is based will always apply, even if the employment contract is governed by English law. Nonetheless the governing law of the contract should also be considered, as should any rights or protections under that contract.

When planning interviews abroad it is crucial that the law and procedure relevant to those jurisdictions are considered. Employment documents should be reviewed to ensure that procedures are followed. It is important to consider whether the employee or employer is covered by any regulatory rules within that jurisdiction (as well as the United Kingdom) to ensure compliance with any reporting obligations.

It would be wise to obtain local legal advice on local laws and culture, which should be factored into the interview strategy. Clearly, interviews should comply with local laws, and in particular those relating to employment, data protection, privacy, privilege and blocking statutes. While the English rules of privilege determine whether privilege applies in this jurisdiction, authorities from other jurisdictions may also have an interest, and advice should be sought on how privilege is determined there.

A witness's procedural rights in the jurisdiction where he or she is based, as well as in the United Kingdom, should also be considered. Compliance with local laws as well as collective consultation and representation rules should be factored in. In addition, the employer should take advice on whether the employee abroad is covered by UK statutory employment rights.

Issues often arise regarding access to documents, particularly where there are restrictions on the movement of information from one jurisdiction to

© Law Business Research 2021

another.[84] Employees may also have a right to access and correct notes and files identifying them.[85] The applicable directives, regulations or rules should be considered in advance to ensure compliance with data protection laws.

See Chapters 5 on beginning an internal investigation and 40 on data protection

Finally, maintaining confidentiality can present particular challenges when interviewing witnesses abroad, and measures should be put in place to ensure that confidentiality remains.

Key points 7.15

Witness interviews are a key part of most internal investigations and can provide vital information for the investigation. Internal investigation interviews can take the form of either preparatory interviews at the outset of an investigation or substantive interviews likely to take place following a review of relevant material.

There can be a tension between the right of a company to investigate allegations of wrongdoing and undertake witness interviews as part of its review, and the expectations of the authorities to be consulted beforehand. Enforcement agencies may seek to restrict how the interviews are conducted or suggest postponement until they have carried out their investigation. Interviews should be conducted so as to minimise the risk of contamination or prejudice.

UK enforcement agencies have stated that a refusal to provide details of the accounts given by witnesses in internal investigations could be construed as unco-operative or a breach of regulatory requirements. The provision of this information and the form in which it would be provided needs to be balanced with the need to ensure confidentiality in an investigation and to maintain legal privilege.

Where a company is investigating allegations of criminal or regulatory misconduct, it is preferable to have lawyers present at interviews to take notes and identify the key risk areas, and to enable confidentiality and for privilege to be asserted, as appropriate. Where external lawyers have been engaged it is preferable for them to conduct the interviews; they often bring (and, importantly, are seen to bring) expertise, objectivity and independence.

Interviews can be recorded in a number of ways: by recording and transcribing the interview; by counsel preparing notes; and with the preparation of a witness statement. UK and overseas enforcement agencies are likely to seek details of the accounts provided, and consideration should be given to ensuring legal privilege is capable of being asserted. How an interview is recorded, the privilege that may attach to that record, and whether or not to provide details of the witness's account will depend on the circumstances of each case.

84 The UK General Data Protection Regulation sets limits on the collection and use of personal data within the United Kingdom and the European Union. The provisions are supplemented by the Data Protection Act 2018 (passed 23 May 2018).

85 Right of access by the data subject: UK General Data Protection Regulation, Article 15.

© Law Business Research 2021

Legal privilege in the context of witness interviews raises a number of complex issues ,and a claim to privilege will be closely scrutinised by the authorities. Notes of interviews with witnesses who fall outside the 'client' group may attract litigation privilege if circumstances allow, but the facts of each case must be carefully considered. Disclosing information relating to witness interviews could result in a waiver of privilege more generally.

When conducting the interview, lawyers should be satisfied that the witness understands the basis on which he or she is being interviewed, its purpose, and the use that could be made of the information provided. While there is no formal requirement to do so, it is best practice for the witness to be given an *Upjohn* warning at the outset and to remind them of confidentiality. Where a company has decided to waive privilege prior to the interview, the *Upjohn* (or similar) warning may need to be strengthened. It is unlikely that a formal caution, similar to that given by the police when investigating suspects, would be required.

The company should consider whether its own legal advisers can give advice to the witness or whether to offer (and to pay for) separate independent legal advice, particularly where there may be a conflict of interest between the company and the witness and where the witness is at risk of criminal or regulatory investigation, or where the company could be implicated in corporate wrongdoing.

In general, a company cannot provide a witness with amnesty from criminal or regulatory action. Similarly an agreement cannot prevent disclosures to regulators or inhibit criminal investigations. Amnesty against internal disciplinary action is rare and while it is possible to agree not to pursue civil claims in return for information being provided, this should generally not be offered until the full facts have been established.

Interviewing witnesses abroad can present particular challenges in global investigations. It is crucial that the law and procedure relevant to those jurisdictions are considered and that any relevant regulatory rules are complied with. Measures should also be put in place to seek to ensure confidentiality.

© Law Business Research 2021

8

Witness Interviews in Internal Investigations: The US Perspective

Anne M Tompkins, Jodi Avergun and J Robert Duncan[1]

Introduction 8.1

The white-collar practitioner's interview of a company employee or officer is often the main event of an internal investigation or review. Significant planning and execution are required, however, well before a lawyer conducts the interview. Whether a witness interview is part of an internal or regulator-facing investigation, or general proactive review, it must be designed to extract the necessary information. Some witness interviews may be designed to gain a level of understanding about business operations or controls present in an organisation, while others may seek to determine corporate or individual culpability after a whistle is blown or an accusation levelled. In each case, the white-collar practitioner must focus his or her planning and resources on uncovering the most relevant information. This chapter provides practical considerations to prepare for, perform and report on witness interviews in the typical white-collar case.

Preparation for the interview 8.2

A good interview process starts with identifying the individuals with potentially relevant information to the investigation. In some cases, as with a specific whistleblower allegation, identifying the right interviewee may be easy. Larger or less well-defined reviews require more planning with respect to identifying the interviewees. One practical way to start is to obtain organisational charts, which will allow the practitioner to see reporting relationships and the relative rank of employees within the organisation. Speaking to a mixture of both high- and low-ranking employees can assist in collecting a broad base of information.

1 Anne M Tompkins and Jodi Avergun are partners and J Robert Duncan is an associate at Cadwalader, Wickersham & Taft LLP.

© Law Business Research 2021

Although attorneys often focus on higher-ranking employers, lower-ranking employees are closer to the day-to-day operations of an organisation and can provide important insight into operations and employee relationships.

Attorneys should be prepared, and even expect, that some employees will not have the knowledge that they are seeking or may not have the expected information. Flexibility is important, as interview time is valuable. If chosen carefully, almost all interviewees will have some valuable information, even if the expected information is not available from a particular interviewee. But, when the interviewee lacks the relevant information, careful consideration should be given to cutting a non-productive interview short to avoid unnecessary costs and to leave time for more substantive conversations later.

Once interviewees are chosen, a practitioner should consider the order in which witnesses will be interviewed. Generally, it is best to start with interviewees who may have background information to gain familiarity with the subject of the investigation and general information about both the industry and the particular practices of the company. Background interviews also help define the parameters of more specific and focused interviews of later witnesses. As the interview schedule progresses, more discrete and specific issues can be the focus. If possible, it is best to interview employees in surroundings that are comfortable to them. However, certain sensitive interviews may be better conducted at a third-party location, such as a hotel conference room nearby to the interviewee's home or office. It is important that interviewees feel comfortable to speak freely and honestly, which may dictate a meeting outside the workspace and away from co-workers and supervisors to avoid the perception of corporate control.

Attorneys usually rely on outlines to guide the interview. An outline will annotate the main issues and information sought and provide a checklist to make sure all planned topics are covered in the interview. Key questions or points can be listed to aid in the interview process and flow. Relevant background information, such as key dates or events, or excerpts from key emails should also be included to aid in the event that an interviewee does not recall important details. In addition, an outline will highlight specific documents or exhibits that will be covered with an interviewee to aid in refreshing the witness's memory or elucidating statements made by the witness. The interviewer should, however, remain nimble and be able to veer 'off script' if unexpected information surfaces during the interview. Preparation is key, but not at the expense of gaining valuable information.

Finally, when preparing for interviews in locations outside the United States, planning for the interview should account for local data-privacy laws and blocking statutes and the need for interpreters. Attorneys should understand before conducting interviews abroad any restrictions on recording interviews and leaving the country with notes taken during an interview. Interpreters should be used unless the interviewee is native-language proficient in the language of the interviewer to avoid any misunderstandings. Because it is likely that the interview will deal with complex and technical subject matter, even highly proficient speakers may struggle with some topics.

© Law Business Research 2021

Upjohn protections 8.3

When a practitioner who represents a corporate client is interviewing an employee, it is important that the attorney ensures that the witness understand the limitations of an attorney's representation and issues surrounding privilege. This is commonly referred to as an *Upjohn*[2] warning, and entails informing the witness that the attorney represents the company, not the witness individually. In addition, the attorney should inform the employee witness that:

- counsel has been hired to gather information for the purposes of providing legal advice to their client – the corporation;
- their fact-gathering is protected by both attorney–client communications and work-product privilege;
- that privilege belongs not to the witness, but to the company, and it is the exclusive decision of the company whether to waive that privilege – which it can do at any time; and
- the witness must keep the interview and what is discussed during it private and confidential.

Following an *Upjohn* warning, attorneys should ensure that the witness understood the warning and extensively document that the *Upjohn* warning was given and understood.

A witness is likely to have questions after being given an *Upjohn* warning – the most common being 'do I need my own attorney?' Attorneys must take care to develop a strategy for responding to such questions. It is not proper for the attorney to provide legal advice to the witness, having just explicitly disclaimed an attorney–client relationship with that individual. If a witness persists in requesting legal advice, an attorney should confer with internal company counsel, who may then offer the employee names of potential attorneys with whom the witness can consult. Telling the witness that they need (or do not need) their own counsel could constitute legal advice, so attorneys should, wherever possible, refrain from doing so.

See Chapter 14 on employee rights

Protecting work-product and attorney–client privilege 8.4

In the United States, there are two main types of privilege that may protect work-product and communications during an internal investigation: attorney–client privilege and work-product privilege. The attorney–client privilege protects communications between an attorney and his or her client to encourage full and frank communication without fear that confidential information will be disclosed to others.[3] Work-product privilege is broader than the attorney–client privilege, but it does not extend to every document generated or

2 See *Upjohn Co. v. U.S.*, 449 U.S. 383, 385 (1981) (stating the privilege protects communications between the client and the attorney, not the underlying facts).

3 *Swidler Berlin v. United States*, 524 U.S. 399, 403 (1998).

© Law Business Research 2021

reviewed by the attorney.[4] Work-product privilege applies to materials prepared in the anticipation of litigation, litigation in process, or the prospect of future litigation, and reflects litigation investigation or analysis.[5]

There are many best practices to protect communications and documents – including notes as discussed more fully below – under both privilege doctrines. First, to establish and document the attorney–client relationship and basis for work-product privilege, the corporation should state in writing that the attorney has been hired to conduct an internal investigation in anticipation of government or civil litigation. Corporations can even include this language in their company policy regarding internal investigations. Secondly, although internal investigations are largely a fact-finding mission, it is important to ensure that there is sufficient attorney oversight and involvement in the investigation, as the overall purpose of an investigation is to render legal advice based on its findings. Even though the privilege can extend to conversations with a non-attorney as long as that person acts as an agent of the attorney, it is always safer to consistently involve corporate and external counsel in these conversations. Counsel should routinely document that the investigation is made to render legal advice and that these communications are privileged and confidential. This can be accomplished by both marking documents as 'Privileged and Confidential' and giving witnesses an *Upjohn* warning, informing them of their relationship to counsel and that all communications are confidential.

See Chapter 37 on privilege

Practitioners conducting investigations outside the United States must be aware of different standards for privilege and adjust accordingly. What may be privileged in the United States may be discoverable in other jurisdictions. For example, in the United Kingdom the attorney–client privilege is limited only to discussions of legal advice between an attorney and his or her client – the 'client' may not include lower-level company employees who do not have the authority to seek and receive legal advice on behalf of the company.[6] In addition, in the United Kingdom legal advice privilege does not extend protection to communications with third parties, even where those third parties, such as accountants, were engaged to assist or enable an attorney to provide legal advice to the client.[7]

See Chapter 36 on UK privilege

8.5 Note-taking and privilege

To ensure that witnesses are comfortable and candid, informal note-taking should be considered. For example, some attorneys find that typing notes on a laptop during an interview is distracting or intimidating to the witness, so

4 *NXIVM Corporation v. O'Hara*, 241 F.R.D. 109, 126-27 (N.D.N.Y. 2007).

5 Fed. R. Civ. P. 26(b)(3); Restatement of the Law, Third, Law Governing Lawyers § 136 – Work Product Immunity.

6 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* (2017) EWHC 1017 (QB) at para. 70.

7 Litigation privilege, however, may apply to communications with third parties, subject to certain conditions being met.

© Law Business Research 2021

lawyers should be ready to handwrite their notes if this would lead to a better interview outcome. While this may increase witness comfort, it decreases efficiency, as such notes are going to have to be typed at a later date. For one or two interviews, this is reasonable, but when interviewing a dozen or more individuals, typing up handwritten notes will be a burdensome task.

Special attention should be paid to how notes are taken for the purpose of discoverability under the work-product privilege doctrine. Under the doctrine, protection attaches to the 'thoughts and impressions' of attorney work-product and these thoughts and mental impressions have often been afforded the strongest protections under the principles of evidence and civil procedure.[8] The decision to take notes as opposed to typing a verbatim transcript carries important implications under these doctrines of which interviewers should be aware before making a decision on their preferred method during an interview. Protecting privilege requires a complicated analysis and varies significantly based on the jurisdiction in which the investigation will occur.

For example, if privilege protection regarding the notes of an interview was challenged, it is less likely – in most jurisdictions – that a court would characterise a verbatim transcript as containing the 'thoughts and impressions' of the attorney. Such a ruling would increase the likelihood of its discoverability.[9] Note-taking including summaries and thoughts, on the other hand, is more likely to contain the thoughts and mental impressions that the attorney has throughout the interview, eliciting work-product protection and making this approach both more helpful to the attorney when reviewing the topics discussed in the interview in addition to reducing the likelihood of discoverability. One approach is to take notes on the same, or slightly modified, document used to create the outline. This approach makes it easier for the note-taker to follow the topics in the interview and notify the interviewer of any missed topics, and increases the likelihood that the note-taker will record thoughts and impressions rather than verbatim conversations.

On the other hand, verbatim transcripts are not necessarily without privilege protection and can certainly be helpful if the investigator knows for certain that they will need to recall exactly what has been said during an interview. Depending on the type of interview being conducted or the type of

8 See *Hickman v. Taylor*, 329 U.S. 495 (1947).

9 Courts across the United States are inconsistent on the protection of verbatim transcripts, even when prepared in anticipation of or during litigation. Therefore, the safest course of action when privilege protection is paramount is to prepare notes that reflect the 'thoughts and impressions' of the attorney taking them. Compare *Nam v. U.S. Express, Inc.*, 2012 WL 12840094, at *3 (E.D. Tenn. 15 May 2012) (holding that recordings of non-party witness interviews were not privileged because they were merely recitations of facts and did not contain mental impressions, conclusions, opinions or legal theories of a party's attorney concerning the litigation), with *Hatamian v. Advanced Micro Devices, Inc.*, Case No. 14-cv-00226-YGR (JSC), 2016 U.S. Dist. LEXIS 60551, at *4 (N.D. Cal. 6 May 2016) (preventing discovery of verbatim interview notes as factual work-product).

© Law Business Research 2021

business taking place at the firm under investigation, certain interviews may be extremely fact-intensive and require greater precision during the note-taking process. For example, if the investigation hinges on the steps and processes employed throughout a complex financial transaction, it may be beneficial to have a full transcript to review the steps and processes in the future. The need for the protection of privilege versus the need for exactness must be weighed.

Immediately following an interview, and before the commencement of the next interview on the schedule, the interviewer and note-taker should confer about the interview, allowing the note-taker – who is usually the more inexperienced party – to jot down any other notes that may be of use at a later date. Once the interviews have concluded for the day, the note-taker should re-review his or her notes, making appropriate edits to allow for the cleaning up of the work-product at a later date. Finally, when all interviews are complete, the note-taker should prepare a clear and concise document that memorialises the contents of the interview and distils all relevant information for easy recall and access.

There is no correct answer for every investigation, and it is up to the interviewer to use his or her best informed judgement when deciding how to take notes through the interview. In most situations, the specific nature of the investigation and the sensitivity of the information will provide sufficient guidance.

8.6 Interactions with witnesses

One of the first challenges that can take place prior to an interview is the consideration of providing counsel for the witness. Often, companies will provide counsel for the witness so that the witness has an advocate and to avoid creating the false impression that the company's counsel is also charged with representing the witness. If both the company under investigation and the specific employee being interviewed are potentially facing criminal charges, it is generally recommended that the employee retain separate counsel in case the interests of the company and individual diverge. Furthermore, the employer and the employee could consent to enter into a joint defence agreement that will facilitate sharing information, based on their common interests in the investigation and defence.

When considering interactions with witnesses, the interviewer should determine whether there is a company policy on co-operation with investigations. Firms may have policies that require co-operation during internal investigation and knowledge of these policies prior to the interview potentially could serve as a helpful starting point. Certain witnesses may be unaware that these policies even exist – which the interviewing attorney may want to bring to their attention should the need arise.

With respect to conducting the interview itself, it is important to tailor the approach according to the particular witness. If a witness is friendly, and not suspected of wrongdoing, it is important to start by being approachable and personable with the witness to avoid any intimidation and potentially evasive or unhelpful answers. The interviewing attorney should begin the interview in a 'light' and non-demanding fashion to put the witness at ease. If the witness

© Law Business Research 2021

does not feel under pressure from direct and pointed questions, then he or she will be much more likely to share information that pertains to the investigation. If, however, an attorney knows that a witness is likely to be adverse or hostile, a different approach may be necessary. Witnesses may be hostile when they have committed a wrongful act – where information from an investigation or previous interviews suggests a witness is culpable. When confronting a witness with documents that show guilt or wrongdoing, conducting a cross-examination with leading questions may be more helpful. Regardless of the witness's posture, the interviewer should also allow for questions from the witness. The goal of the interview process is to allow the witness to 'tell their story' while allowing the interviewer to maintain the role of counsellor and listener. Receiving and responding to the witness's questions thoughtfully and respectfully will quickly establish trust and confidence, as opposed to coldness and hostility.

In addition to allowing the witness to 'tell their story', one of the other major objectives of an interview is to ask the witness about other individuals who may have knowledge on the subject of the investigation. When a witness is describing a certain set of events, it is not uncommon for him or her to discuss conversations held with others as these events took place. The interviewer should make sure to follow up on the other individuals that the witness brings up, both in the interview itself and after deciding who else should be contacted as a new witness.

Because each witness will react differently to certain questions, and there is no set formula for conducting an interview, the interviewers should strive to make the interview as open and conversational as possible while ensuring that the information being shared is both relevant and helpful to the investigation as a whole.

Document review and selection 8.7

In the ideal case, a white-collar practitioner will only conduct an interview of a company witness after a comprehensive document review has been conducted. Of course, some interviews are purely fact-finding and take place in emergent situations, making pre-interview document review unlikely. However, often, the review process should be under way, or ideally, completed before interviews take place.

The key dates and types of documents (e.g., emails, phone logs, text messages and financial documents) must be determined. These parameters will be set based on the type of information sought and the interviewees to be selected.

See Chapter 11 on production of information to authorities

Remote interviews: costs and covid-security 8.8

Covid-19 has impacted many types of legal work, including investigations and witness interviews. Remote interviews have become the norm – and are likely to remain so for the foreseeable future. Even US government agencies are conducting interviews remotely. Not being in the same room as the interviewee creates challenges for attorneys, relating to, among other things, logistics, the evaluation of credibility and security.

© Law Business Research 2021

Even before pandemic-related lockdowns began in early 2020, many clients preferred that attorneys performed interviews via videoconference to reduce costs. Attorneys that have performed remote interviews are well aware of the limitations imposed by not being present with the interviewee. For example, if it is necessary to show a witness documents and exhibits during the interview, the logistics can be difficult. To address these logistical hurdles, several platforms have been developed that allow for remote depositions and interviews. For example, many companies have developed platforms that aim to provide a seamless interface for remote depositions – allowing for document sharing and a host of features, such as private chat between members of an interview team to alleviate some of the issues faced when everyone is not in the same room. These platforms, although designed for deposition, are also a good option for witness interviews in internal investigations.

Regardless of the technology used, however, videoconference interviewing may still lead to a less effective interview – especially in the immediate future where attorneys are still used to travelling and performing interviews in the same room with the interviewee. Conducting an interview in person allows the interviewer to view and interpret attitude and body language in real-time. In-person interviewing also allows the interviewer to develop a rapport with the interviewee that is usually not possible over video link. It is also likely that a witness will have a harder time being untruthful, evasive or hostile in person than through a video screen. And it is much more difficult to assess an interviewee's credibility from miles away, no matter how good the high-definition screens are. The more important the interview, the more likely an in-person interview may need to be conducted where possible. A proactive review of internal control processes is a better candidate for a telephone or video meeting than an internal investigation designed to ferret out wrongdoing.

The best cost-control and social-distancing measure, though, is still effective and meticulous planning. By focusing only on relevant interview topics, some interviews can be shortened or even forgone.

8.9 Reporting the results of interviews

Often the format and type of report for an interview will be determined by the client in advance of any interviews. In large investigations, shorter decks or slides may be more helpful to allow the client to digest large amounts of data from various jurisdictions. These decks should include all pertinent information obtained from interviews as well as data on the number, location and type of interviews. Whether a more summarised slide deck with bullet points, or a more in-depth memo is prepared, the attorney should highlight significant findings and recommendations for next steps and further action.

Especially when preparing less detailed investigation reports, an attorney should schedule time with the client to go through the report and elaborate on key findings and recommendations. The attorney and client must be aligned on the next steps to ensure the best outcome from the investigation and interviews.

© Law Business Research 2021

Conclusion 8.10

A well-done witness interview in a white-collar case can assist the client in determining case strategy, assessing damage, and uncovering or hopefully disproving wrongdoing. Careful scoping will ensure a focused and cost-efficient interview. Understanding at the outset what the goal of the interview is, as well as local laws and practices that might hinder attaining that goal, will avoid unnecessary hurdles and produce the result that is best for the case.

© Law Business Research 2021

9

Co-operating with the Authorities: The UK Perspective

Matthew Bruce, Ali Kirby-Harris, Ben Morgan and Ali Sallaway[1]

9.1 Introduction

This chapter focuses on corporate co-operation with regulatory agencies and criminal authorities: where and when co-operation is required, its outcomes and its implications. It looks at the expanding meaning of 'co-operation', current practice and guidance and recent jurisprudence.

Where co-operation is mandatory, the corporate has no option but to comply, or face criminal or disciplinary sanction. A few non-exhaustive examples of mandatory co-operation in the United Kingdom are where:

- there is a warrant to enter and search premises, and to seize material found therein;
- a court issues a witness summons for a representative of the corporate to attend court, often with documents; or
- a compelled notice is issued, requiring the recipient to provide information or documents, or to attend for interview.

Where co-operation is voluntary, the debate becomes more interesting. Generally, there is an increasing expectation that corporates should co-operate with investigations. Co-operation can be beneficial for a number of reasons (for example, it can result in a less serious outcome, help to mitigate sentences or sanctions in the event of a successful prosecution or enforcement, or enable an early decision to take no further action to be reached). It will be relevant at every stage of engagement with regulators, or other enforcement authorities, and can help to limit costs to the business and give the corporate some

1 Matthew Bruce, Ali Kirby-Harris, Ben Morgan and Ali Sallaway are partners at Freshfields Bruckhaus Deringer LLP.

© Law Business Research 2021

influence over the course of an investigation. A collaborative approach may also enable a corporate to manage publicity and communications in conjunction with the authority, and limit reputational damage.

9.2 The status of the corporate and other initial considerations

The status of the corporate is key. Is it a victim or a witness? Is it the target or subject of the investigation? If a witness, is it at risk of becoming a subject? Understanding status is essential to providing proper, informed guidance.

Establishing the status of the corporate at the outset of an investigation, if possible, enables the evaluation of potential liability, including if the corporate is exposed to risk and the potential mitigating benefits of co-operation. This evaluation should define how the approach to the authority is made and how the relationship is managed.

If the corporate is a witness, it may be subject to mandatory co-operation requirements, such as compelled requests for information. While proactive co-operation may enhance a corporate's relationship with its regulator or enforcement body, and be consistent with its corporate governance values, a corporate may have good reasons to be circumspect in dealings with the authorities in an investigation. For example, a corporate witness may have an ongoing commercial relationship with the corporate suspect (such as an auditor–client relationship), meaning the corporate witness will need to consider its obligations to the client and potential exposure to litigation or investigation resulting from disclosure. A corporate may also evolve from witness to suspect over time.

Beyond mandatory obligations, there is also a discretionary element to the type of co-operation that might be appropriate for a corporate to consider providing, and there are different drivers behind this – legal, tactical, practical and even 'ethical'. The court suggested in the *Amec Foster Wheeler Energy Limited (AFWEL)* deferred prosecution agreement (DPA) that self-reporting is 'a matter of ethical corporate governance' and that there is a 'moral duty on all citizens in this respect which extends at least equally to corporations'.[2] This DPA judgment is the first to indicate a moral standard for self-reporting above and beyond the requirements of the law and outside the context of penalty reduction (albeit in *obiter*).

The desire or need to co-operate may trigger an internal investigation to preliminarily establish the facts and veracity of the allegations. While not the only factor influencing the approach to take, corporates must consider whether the authorities would want or expect involvement in setting the scope of an internal investigation. This is discussed below in more detail. The corporate

2 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021], paras. 19–20.

© Law Business Research 2021

should also be mindful of any mandatory reporting or disclosure obligations that arise as it gains further information relating to the allegations.[3]

Other initial considerations include legal privilege – asserting such privilege where appropriate but balancing it with certain authorities' desire to review first accounts of witnesses. This is discussed in more detail later in the chapter.

See Chapter 36 on privilege

Where possible, the strength of the known evidence should be assessed as quickly as possible. Information obtained by a prosecutor during an investigation is generally admissible in criminal proceedings against the corporate, so it is important to have regard to the potential effects of any documents or information voluntarily disclosed and the extent to which co-operation may undermine any potential defences the corporate may later wish to mount.[4] It is also important to try to understand what evidence might arise in the investigation (other than that known to the corporate), so that a broader assessment of potential exposure can be made.

9.3 What does co-operation mean?

9.3.1 Definition and descriptions

Increasingly, co-operation is a more nuanced concept than a traditional guilty plea and an offer to give evidence on behalf of the prosecution: it involves self-reporting, acting in a manner that saves the authority's time and resources, a willingness to cede a good deal of control in internal investigations, voluntary disclosure of gathered evidence, and genuine and consistent transparency – all factors referred to by courts and authorities.

Multiple authorities have stressed the importance of genuine co-operation. In August 2019, the Serious Fraud Office (SFO) published an extract of its operational handbook entitled Corporate Co-operation Guidance, which provides guidance to SFO prosecutors on how to assess corporate co-operation.[5] This lists several dozen 'indicators of good practice' that the SFO may take

3 Obligations may arise under the Proceeds of Crime Act 2002, Part 3 of the Terrorism Act, or any reporting obligations that may arise under the UK's financial sanctions regime, particularly for entities in the 'regulated sector'. Further, listed companies will need to consider their disclosure obligations to the market, such as Part 7 of the Financial Services Act 2012 and the EU Market Abuse Regulation and the Market Abuse (Amendment) (EU Exit) Regulations 2018.

4 Material described in para. 13(6) of Schedule 17 of the Crime and Courts Act 2013 can only be used in limited circumstances but there is no limitation in the use to which other material obtained by a prosecutor during the DPA negotiation period may be put against the corporate or anyone else so far as the rules of evidence permit. See the Deferred Prosecution Agreements Code of Practice (DPA Code of Practice), paras. 4.4 and 4.5 (link to download Code of Practice at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/).

5 SFO Operational Handbook, Corporate Co-operation Guidance (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/).

© Law Business Research 2021

into account when assessing whether a corporate is genuinely co-operative. Importantly, the list is neither exhaustive nor prescriptive: the SFO acknowledges that each case will be different.

As a summary, the Corporate Co-operation Guidance notes:

> *Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrongdoing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.*
>
> *Genuine co-operation is inconsistent with: protecting specific individuals or unjustifiably blaming others; putting subjects on notice and creating a danger of tampering with evidence or testimony; silence about selected issues; and tactical delay or information overloads.*[6]

Various other authorities have similarly stressed the importance of corporate co-operation by the entities they are investigating, including, for example, the Information Commissioner's Office (ICO), which can impose fines for data protection breaches, and the Financial Conduct Authority (FCA).[7]

Genuine and continual co-operation 9.3.2

Authorities expect co-operation to be genuine, proactive and continual.[8] When a resolution of an investigation is under consideration, a dominant public interest factor against prosecution is co-operation. Considerable weight is given to a 'genuinely proactive approach' by a corporate that becomes aware of potential offending.[9] If an investigation is to be resolved by way of a DPA,

6 ibid., p. 1.

7 ICO, Regulatory Action Policy, p. 24 (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf); FCA Handbook, EG 2.12 (*Co-operation*).

8 For instance, the FCA considers that a firm's pattern of co-operation during the period leading up to the investigation, as well as during the investigation itself, is relevant. The FCA Handbook notes: 'An important consideration before an enforcement investigation and/or enforcement action is taken forward is the nature of a firm's overall relationship with the FCA and whether, against that background, the use of enforcement tools is likely to further the FCA's aims and objectives. So, for any similar set of facts, using enforcement tools will be less likely if a firm has built up over time a strong track record of taking its senior management responsibilities seriously and been open and communicative with the FCA' (FCA Handbook, EG 2.12.1). The Competition and Markets Authority (CMA) similarly requires continuous and complete co-operation as well as refraining from further participation in cartel activities (https://www.gov.uk/government/publications/leniency-and-no-action-applications-in-cartel-cases and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf).

9 DPA Code of Practice, para. 2.8.2; FCA Handbook, EG 2.12.1.

© Law Business Research 2021

then the public interest will be a focus of the court in its assessment of the proposed agreement.

Co-operation will clearly be considered in the context of the corporate's general attitude towards the investigation. Companies that make incorrect or unsubstantiated arguments about the underlying nature of the misconduct run a real risk of being deemed unco-operative, while companies that fully co-operate can earn significant leniency in terms of the eventual disposal of a matter, whether that entails entirely extinguishing, or at least reducing, monetary and other penalties. This point was highlighted by the reported conduct of Sweett Group: the company was heavily criticised by the SFO and the court for attempting to 'divert the attention of the SFO away from further enquiry of the contract' under scrutiny by attempting to obtain a letter characterising the offending payment its subsidiaries had made as a legal finder's fee under United Arab Emirates law.[10] On the other hand, in the *Rolls-Royce* case, the SFO offered, and the court approved, for the first time, a DPA with a 50 per cent discount to the monetary penalty that would otherwise have been required. This represented the one-third discount that is the equivalent of what is usually available for an early guilty plea plus an additional 16.7 per cent discount in recognition of Rolls-Royce's 'extraordinary cooperation'.[11] The SFO has agreed to a similar level of discount in several DPAs since *Rolls-Royce*. The Office of Financial Sanctions Implementation (OFSI) within HM Treasury, which has powers to impose potentially significant monetary penalties on companies and individuals for breaches of financial sanctions law, mirrors this approach, noting in its guidance that if 'we discover that parties have dealt with us in bad faith and if the case is not criminally prosecuted, we will normally impose a monetary penalty'.[12] The ICO will also take into account the level of co-operation shown by a corporate when deciding on enforcement, and (as discussed further below) corporates may be subject to greater penalties if they fail to co-operate fully with an ICO investigation.[13]

As mentioned previously, the *AFWEL* DPA[14] has introduced new language concerning the morality of self-reporting, providing further complexion on what 'co-operation' really means. Many companies already have in place processes designed to encourage reflection at the most senior levels of management. These processes typically promote consideration as to whether to

10 *R v. Sweett Group*, Sentencing Remarks.

11 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 19.

12 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/605884/Monetary_penalties_for_breaches_of_financial_sanctions.pdf).

13 An instructive example of the ICO's tough approach is the £400,000 fine and criminal penalty handed to Keurboom Communications after Keurboom failed to comply with an information notice regarding a breach of the Privacy and Electronic Communication Regulations.

14 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021].

© Law Business Research 2021

self-report potential criminal conduct that may be identified internally through whistleblowers or otherwise.

Self-reporting 9.3.3

The SFO, FCA, OFSI, ICO and the Competition and Markets Authority (CMA) have all indicated that a corporate should self-report as promptly as possible to be considered to be co-operating.[15] How early a corporate does so is a factor the regulators and enforcement authorities will consider when deciding how to handle the matter, including what kind of resolution is an appropriate outcome.[16] However, regulators and enforcement authorities generally do not expect corporates to report all allegations of criminal behaviour as soon as they become aware of them, so a balance needs to be struck.[17] Allegations need to be considered and verified to a certain extent before any potential self-report occurs. For the SFO, reporting wrongdoing but failing to verify it or believing it is inaccurate or incomplete is a factor in favour of prosecution or higher sanctions.[18] The level of investigation that is required to 'verify' wrongdoing is undefined and is an often difficult judgement call for the corporate and its advisers.

When considering a self-report, regulators and authorities consider the information provided, and the time at which the corporate came forward, to assess whether it was voluntary and complete – generally, disclosure will not be considered voluntary if regulators have already required documents or the corporate knows that an investigation is imminent.[19] Of course, not all regu-

15 See, e.g., 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021, para. 3.28. For example, the OFSI reduced the fine imposed on Standard Chartered Bank for breaches of financial sanctions by 30 per cent in light of the bank's voluntary disclosure: OFSI Imposition of Monetary Penalty – Standard Chartered Bank (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf). For the ICO's position, see ICO, Regulatory Action Policy, p. 24 (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf). For the FCA's position, see the FCA Handbook, EG 2.12.1.

16 DPA Code of Practice, para. 2.9.2.

17 For the SFO's position, see a speech by Lisa Osofsky, SFO Director, at the Royal United Services Institute in London, 3 April 2019 (https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/). The FCA 'expect firms to be able to judge how serious a problem is and where it falls on a continuum between urgent notification and potentially no need to tell us at all' (speech by Jamie Symington, 5 November 2015, https://www.fca.org.uk/news/speeches/internal-investigations-firms). The OFSI notes that breaches should be disclosed 'as soon as reasonably practicable after discovery' and that 'it is reasonable for a person to take some time to assess the nature and extent of the breach, or seek legal advice' ('Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021, para. 3.32).

18 DPA Code of Practice, para. 2.8.1(vi).

19 SFO prosecutors must consider 'the totality of the information that the Company has provided, the extent to which the offending was previously known, if at all, to the SFO, and the

© Law Business Research 2021

lators or enforcement authorities take the same approach to assessing these factors: for example, the OFSI may give credit even when the entity was not the first to voluntarily report the activity, whereas the CMA requires a potential cartel member expecting leniency to be the first member to report the potential wrongdoing.[20]

Companies should therefore consider the following factors if they wish to maximise their co-operative stance:

- where possible, the alleged criminal conduct should be reported to the regulator or relevant enforcement authority before it otherwise becomes aware of it. A corporate should consider the possibility of whistleblowers and be aware of reports to other authorities in the United Kingdom or overseas;
- the corporate is entitled to conduct an 'initial assessment' of the allegation. However, as soon as reasonable grounds to suspect wrongdoing are identified, there is an expectation that these will be flagged;[21] and
- the extent to which a corporate involves the prosecutor in the early stages of an investigation is a relevant factor in assessing co-operation.[22]

On the DPA front, although the failure of a corporate to self-report is not necessarily a bar to DPA negotiations, it must be considered when assessing whether

---

extent to which the Company is providing it voluntarily, that is without the threat of imminent disclosure by a third party or compulsion' (see the guidance for prosecutors on DPAs in the SFO's Operational Handbook). The OFSI 'will consider the facts and timing of each disclosure individually' but does not consider disclosure to be voluntary if it comes after it or other regulators have used their powers to compel disclosure of information or if 'the person has been prompted to disclose the facts because OFSI is assessing a case' ('Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021, para. 3.35).

20 https://www.gov.uk/government/publications/leniency-and-no-action-applications-in-cartel-cases and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf.

21 SFO Operational Handbook, Deferred Prosecution Agreements (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/); see, e.g., Lisa Osofsky's speech of 3 April 2019. 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021, para. 3.32.

22 See DPA Code of Practice, para. 2.9.2. For example, in the *Standard Bank* case, the alleged misconduct was reported 'within a matter of days of it coming to its attention' (*SFO v. Standard Bank plc*, Statement of Facts prepared pursuant to para. 6(1) of Schedule 17 to the Crime and Courts Act 2013, para. 4). The court noted that considerable weight was to be attached to the swift and proactive self-reporting (*SFO v. Standard Bank plc*, Approved Judgment, (Case No. U20150854) [2016] Lloyd's Rep FC 102, para. 27). In *Sarclad*, after unearthing concerns, Sarclad took immediate action by retaining a law firm to undertake an independent internal investigation and a self-report came six weeks later. The court commended this promptness and co-operation (*SFO v. Sarclad Ltd*, Approved Judgment, (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509, para. 11).

© Law Business Research 2021

a DPA is in the public interest.[23] In the absence of self-reporting, a corporate is likely to need to make up lost ground by demonstrating significantly more subsequent co-operation to earn a comparable degree of leniency. In the *Rolls-Royce* case, there was no self-report at the outset but 'extraordinary' co-operation was offered during the investigation, resulting in the SFO and the court giving the same degree of leniency in the DPA as if Rolls-Royce had self-reported.

Conducting an internal investigation with SFO or FCA approval 9.3.4

Following a self-report, the SFO or FCA expects genuine and constructive co-operation, meaning any internal investigation should be approved by, and done in conjunction with, the relevant enforcement agency.[24] It is likely the enforcement authority will want to have a reasonable degree of involvement in the early stages of an internal investigation. For example, the SFO expects to be able to discuss work plans, timetabling, interviewing and actions regarding personnel, and to give directions (for example, relating to data capture and processing) and 'other overt steps'.[25] Both the SFO and FCA will expect the corporate to provide a copy of any internal investigation report, including source documents.[26]

SFO expectations on data handling 9.3.5

The SFO has expressed particular concern that relevant data is properly preserved. For example, its Corporate Co-operation Guidance advises companies to ensure that the digital integrity of material is preserved, to identify the reasons for any data loss, deletion or destruction, and to create and maintain an audit trail on the acquisition and handling of data. Preserving the integrity of data (and later collecting it) may require a significant effort. Companies may consider evaluating, in advance of any investigation, what data sources they have and how they are stored and accessed.[27] For example, the assistance provided

23 SFO Operational Handbook, Deferred Prosecution Agreements, footnote 15 (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/).

24 For the SFO, see DPA Code of Practice, para. 2.9.2. For the FCA, see a speech by Jamie Symington, 5 November 2015 (https://www.fca.org.uk/news/speeches/internal-investigations-firms).

25 For the SFO, see DPA Code of Practice, para. 2.9.2, and Corporate Co-operation Guidance. For the FCA, see a speech by Jamie Symington, 5 November 2015 (https://www.fca.org.uk/news/speeches/internal-investigations-firms).

26 SFO Operational Handbook, Deferred Prosecution Agreements (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/).

27 Where providing data voluntarily to the SFO or when dealing with overseas data, a corporate will have to consider the applicable data privacy laws and take steps accordingly. This may involve proactive and early engagement with the SFO on any potential limitations to the corporate's ability to provide the SFO with the expected data.

© Law Business Research 2021

by Standard Bank included providing documents from email servers held in Africa, inboxes, hard drives and shared drives, paper files, CCTV images and recordings of telephone calls.[28] This material would otherwise have been inaccessible to the SFO. (Further examples are Sarclad, Rolls-Royce and Airbus.[29]) Note also that the Corporate Co-operation Guidance notes that co-operation may involve providing material from overseas when it is in the possession or control of the organisation, as well as identifying and facilitating access to data held by third parties.

9.3.6 Facilitating access to witnesses

See Chapter 3 on self-reporting to authorities

The SFO has also expressed particular concern that 'first accounts' from witnesses are not prejudiced.[30] Other regulatory and enforcement authorities, including the FCA, are increasingly adopting a similar stance.

From a prosecutor's perspective, achieving evidence that will perform at trial is a key principle in a criminal prosecution. The first account of a witness is crucial, and the circumstances in which it is obtained can be critical to the credibility and efficacy of the evidence in a trial. Discrepancies between a first account and subsequent testimony, or being unable to demonstrate consistency (i.e., if the prosecutor cannot produce a first account), can undermine the prosecution case. As such, the SFO places particular significance on obtaining first access to witnesses, or to notes or summaries of first accounts. In certain circumstances, the SFO or the FCA may expect corporates not to interview witnesses before consulting the relevant authority,[31] or they may request that a corporate does not interview potential witnesses before a compelled interview has been carried out or a witness statement obtained. Where a corporate is able to interview witnesses, the SFO or the FCA may wish to have a say in how the interview is carried out, and to receive copies of any work-product generated following each interview.

---

28 *SFO v. Standard Bank plc*, Statement of Facts prepared pursuant to para. 6(1) of Schedule 17 to the Crime and Courts Act 2013, para. 4.

29 Similarly, Sarclad identified and provided relevant information, such as email caches, that extended the investigation beyond the SFO's original scope (*SFO v. Sarclad Ltd*, Approved Judgment, (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509). Rolls-Royce agreed to provide the SFO with unfiltered access to its records – some 30 million documents – and permitted the SFO to conduct its own digital review to identify potentially privileged documents (*SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249). Similarly, Airbus collected more than 30 million documents and assisted in the prioritisation of documents (*SFO v. Airbus*, Approved Judgment (Case No. U20200108), [2020] 1 WLUK 435, para. 74).

30 DPA Code of Practice, para. 2.9.3.

31 Corporate Co-operation Guidance, Preserving and providing material, para. 6(i). Further, the court in *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 20(i)) cited Rolls-Royce's deferring of internal interviews until the SFO had first completed its interviews as evidence of their co-operation with SFO.

© Law Business Research 2021

The SFO will also expect co-operating companies to make employees and (where possible) third parties available for SFO interviews, including arranging for them to return to the United Kingdom if necessary.

Privilege 9.3.7

The legal professional privilege often applying to communications generated during an investigation has been a focus of regulators in recent years, especially the SFO, particularly in relation to interview notes. Public statements by the SFO make clear that it considers as a 'significant mark of co-operation a company's decision' to waive privilege over notes of witness interviews.[32] Rolls-Royce received credit for voluntarily disclosing, with limited waiver of privilege, memoranda from more than 200 interviews conducted as part of its internal investigation.[33]

Standard Bank and Sarclad, on the other hand, are understood not to have provided notes (or referred to first-account witness interviews) in their internal investigation reports to avoid waiving privilege, instead providing oral summaries. However, the decision in *R(AL) v. SFO*[34] demonstrates the difficulties that can arise for the SFO from this approach. The court made plain its view that the SFO had not complied with its duty, as a prosecuting authority, to take further steps to obtain witness interview notes so that they may be disclosed in the criminal proceedings in accordance with the defendant's right to a fair trial under Article 6 of the European Convention on Human Rights. The SFO was required to 'assess claims for privilege properly and not cursorily and superficially'.[35]

Further, in *Director of the SFO v. ENRC*, the SFO initially successfully challenged claims of privilege over various documents produced during ENRC's internal investigation and subsequent engagement with the SFO.[36] However, this decision was overturned on appeal on the basis that the interview notes and other materials (including the work-product of forensic accountants) were protected by litigation privilege.[37] The Court of Appeal found that criminal

32 See speech by Lisa Osofsky, Director of the SFO, 3 April 2019.

33 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 20(ii).

34 *R(AL) v. SFO* and others [2018] EWHC 856 (Admin).

35 There have been a number of high-profile decisions in relation to interview notes that have led to substantial development of this topic. For example, in the 2016 *RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch), the High Court rejected claims of legal advice privilege over memoranda of employee interviews prepared by the bank's lawyers, as 'client' was interpreted to cover only those individuals authorised to seek and receive advice from the lawyers. The employees interviewed by the lawyers were thus not considered to be 'clients' of the bank's lawyers. The FCA has also noted that the practice of reading out notes instead of providing written documents is 'unhelpful and unwelcome' – speech by Jamie Symington, 5 November 2015 (https://www.fca.org.uk/news/speeches/internal-investigations-firms).

36 *SFO v. ENRC* [2017] EWHC 1017 (QB) (8 May 2017).

37 *Serious Fraud Office v. Eurasian Natural Resources Corporation* [2018] EWCA Civ 2006.

© Law Business Research 2021

proceedings were sufficiently contemplated for litigation privilege purposes at the time ENRC commenced its internal investigation, and they were definitely contemplated when the SFO subsequently contacted ENRC about the same matter. Note that the dominant purpose test for litigation privilege will still apply.[38]

As a matter of principle, maintaining a proper assertion of privilege should be a 'neutral' factor as far as obtaining credit for co-operation is concerned. The DPA Code of Practice recognises that there is nothing in the existence of the DPA process that alters the fact that privilege is a fundamental right.[39] However, the Court of Appeal in *ENRC* did note that an examination of a corporate's co-operation, for the purposes of determining whether a DPA would be in the interests of justice, 'will consider whether the company was willing to waive any privilege attaching to documents produced during internal investigations, so that it could share those documents with the SFO'. In practice, therefore, the SFO may consider waiving privilege over certain documents to assist the SFO as a sign of co-operation, and so that is a factor that a corporate ought to take into account in its overall engagement.

See Chapter 36 on privilege

The language of the Corporate Co-operation Guidance is particularly strong on privilege, signalling that the SFO is continuing its robust stance on assessing (and challenging) corporates' claims of privilege. The Guidance establishes two new procedural expectations for companies seeking to assert privilege: first, to provide certification by independent counsel supporting any claim of privilege; and second, to provide 'privilege logs' itemising each document withheld on the basis of privilege and the basis on which each is privileged. Although time-consuming and expensive, these new procedures may signal that, if the steps are taken, there is a clearer path for a corporate to assert privilege while maintaining a co-operative stance.

When considering co-operation in the context of a DPA, the Corporate Co-operation Guidance suggests the SFO will expect the corporate to disclose 'witness accounts' and documents shown to witnesses.[40] It also includes a new express expectation that companies seeking co-operation credit should also provide any recordings, notes and transcripts of witness interviews and identify a witness who is competent to speak about the content of each interview.

The Corporate Co-operation Guidance states that companies that retain a legitimate claim to privilege over witness material will not be penalised for asserting privilege (where supported by an independent certification). That said, it is not yet clear whether the SFO will expect such companies to work harder in other areas to 'make up' for lack of credit they would otherwise have

38 Note that in the *ENRC* case, the investigation of the allegations in question was initially framed in contemporaneous documents as being for 'corporate governance reasons', but the Court of Appeal still found that the dominant purpose was to investigate the facts so the corporate could defend the proceedings that were reasonably contemplated at the time.

39 DPA Code of Practice, para. 3.3.

40 ibid., para. 2.8.2(i).

© Law Business Research 2021

received. On the other hand, the SFO has emphasised that it will view the waiver of privilege as a 'strong indicator of cooperation' and an 'important factor' in deciding whether to offer a DPA.[41]

In respect of the regulated sector, the FCA has also highlighted the importance of sharing privileged information generated in internal investigations to be considered co-operative, recognising 'the needs and the right of firms to claim and protect their rights to legal privilege where appropriate' but stressing that 'it should be possible to strike the right balance' and share appropriate documents with the FCA.[42]

Highlighting exculpatory material to the SFO 9.3.8

In recent years, the SFO has emphasised the importance of holding individuals accountable for criminal behaviour. The Corporate Co-operation Guidance repeats this overarching objective. It also articulates a new and controversial expectation that a co-operative corporate will also assist the SFO in identifying documents or information capable of assisting a potential accused or undermining the case for the prosecution (typically called 'exculpatory material').

Co-operation can lead to reduced penalties 9.4

Co-operation with authorities in criminal cases has always been rewarded with a more lenient sentence for a defendant. Conversely, attempts to conceal misconduct may result in a more severe sentence.[43]

See Chapter 25 on fines, disgorgement etc.

Individuals who plead guilty and offer significant voluntary co-operation with a prosecutor may also be entitled to a lesser sentence under section 73 of the Serious Crime and Police Act 2005 (SOCPA).[44] A defendant enters into an agreement with the authorities under SOCPA to provide certain assistance, the extent and nature of which is taken into account when he or she is sentenced. The assistance is often directed at obtaining evidence about other individuals or establishing facts that advance the investigation.

The likelihood of prosecution and the likely sanction in the event of conviction are important factors in any decision to co-operate voluntarily, as there is no guarantee that it will result in a reduced sanction or complete immunity. The corporate and its advisers should always remember that, where there are allegations of criminal offences or regulatory breaches, the regulatory and enforcement bodies' primary role is to properly investigate and prosecute or otherwise

41 Speech by Lisa Osofsky, Director of the SFO, on 3 April 2019.

42 Speech by Jamie Symington, 5 November 2015 (https://www.fca.org.uk/news/speeches/internal-investigations-firms).

43 See, for example, 'Fraud, Bribery and Money Laundering Offences – Definitive Guideline', 1 October 2014, p. 50.

44 This applies when an offence specified under the Schedule to SOCPA has been committed. Prosecutors holding SOCPA powers include the Crown Prosecution Service (CPS), FCA and SFO. See also CPS Guidance on SOCPA: http://www.cps.gov.uk/legal/s_to_u/socpa_agreements_-_note_for_those_representing_assisting_offenders/.

© Law Business Research 2021

sanction the offender. Consideration should also be given to what the overall impact of a particular outcome might be. For example, while a DPA is likely to result in a lower financial penalty than a conviction at trial, it is also likely to entail additional obligations (such as future co-operation, future self-reporting and compliance programme upgrades and assurance) that are not otherwise available as sanctions.

As noted, co-operation with the SFO can result in leniency in penalties. In respect of DPAs, the more serious the offence, the less likely it is that a DPA (as opposed to prosecution) will be considered to be in the public interest. However, in the *Rolls-Royce* case, the court acknowledged that, notwithstanding the gravity of the wrongdoing, on the right terms it was in the interests of justice to resolve the conduct by way of a DPA rather than a trial.[45] Nevertheless, the legislation requires any financial penalty that forms part of a DPA to be broadly comparable to a fine that the court would have imposed following a guilty plea.[46]

Analysis of recent judgments suggests that a 50 per cent reduction can typically be expected in return for broad and effective co-operation from the outset (this has been the case in seven of the 10 DPAs published to date).[47] However, the discount may be lower – for instance, if full co-operation came 'relatively late in the day',[48] or when there are a myriad of aggravating and mitigating factors that may need to be taken into account. For example, the *AFWEL* DPA involved a more complex discount process. Figures for compensation and disgorgement were added together to calculate a 'harm figure' that formed the basis of the fine. In accordance with guidelines for magistrates' courts published by The Sentencing Council for England and Wales,[49] multipliers in respect of aggravating and mitigating factors were then applied to the 'harm figure' to calculate the fine. The total financial penalty comprised the fine, disgorgement

45 *SFO v. Rolls-Royce*, Approved Judgment (Case No. U20170036) [2017] Lloyd's Rep FC 249, paras. 61–64.

46 Crime and Courts Act 2013, Schedule 17, para. 5(4).

47 See, for example, the *Rolls-Royce* case in which the SFO offered, and the court approved, a DPA with the one-third discount that is the equivalent of what is usually available for an early guilty plea plus an additional 16.7 per cent discount in recognition of Rolls-Royce's 'extraordinary co-operation' (*SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 19). Note that the SFO announced two further DPAs in July 2021. However, further details as to the relevant companies or the terms of the DPAs have not yet been made publicly available.

48 'The 40 per cent discount reflects the delayed nature of G4S C&J's substantial cooperation with the SFO's investigation' (https://www.sfo.gov.uk/2020/07/17/sfo-receives-final-approval-for-dpa-with-g4s-care-justice-services-uk-ltd/).

49 See Magistrates' Court Sentencing Guidelines, 'Corporate offenders: fraud, bribery and money laundering', Sentencing Council (https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/corporate-offenders-fraud-bribery-and-money-laundering/).

© Law Business Research 2021

and compensation figures.[50] Co-operation with authorities in the regulated space can have a similar effect on the level of penalties imposed.[51]

That co-operation can lead to reduced penalties is not limited to the SFO. In the regulated space, although regulated persons are legally required to co-operate with the FCA, proactive co-operation can also lead to reduced penalties. This can include not pursuing enforcement action,[52] reduced charges or lighter sanctions. The FCA's Enforcement Guide makes clear that the settlement discount scheme allows a reduction in a financial penalty or period of suspension, restriction or condition that would otherwise be imposed, if agreement is reached at an early stage.[53]

Further, the CMA also operates a leniency regime for self-reporting and co-operating cartel members; the OFSI considers voluntary self-reporting and good-faith co-operation when deciding the level of any penalty (including a potential penalty reduction of up to 50 per cent);[54] and the ICO states that failure to co-operate is an aggravating factor when assessing penalties.[55]

In some cases, the authority in question may have the choice whether to pursue a criminal or civil (or regulatory) outcome (the FCA in relation to

50 In *SFO v. Petrofac Ltd*, where the court followed a similar approach, it listed co-operation as a mitigating factor for calculating the multipliers applied to the harm figure, but noted that 'there was no voluntary or early admission' and that there was a large number of aggravating factors. The court therefore applied a higher multiplier than the default starting point. The harm figure was then reduced under the totality guidance in the Magistrates' Court Sentencing Guidelines (https://www.sentencingcouncil.org.uk/overarching-guides/magistrates-court/item/totality/), for which Petrofac's co-operation was not a relevant factor. Finally, the court applied the usual one-third discount for a guilty plea (*SFO v. Petrofac Ltd*, Sentencing Remarks).

51 See, for example, the FCA's Enforcement Guide and the CMA's guidance on self-reporting cartel conduct.

52 See FCA Handbook, EG 2.1.4.

53 FCA procedure also allows a firm to settle aspects of a case and achieve a discount in respect of those aspects, while continuing to contest other aspects of the case. Timetables for settlement discussions will be set for efficiency and effectiveness and the FCA will expect firms and others to give it all reasonable assistance in this regard.

54 For the OFSI, see 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2021 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/605884/Monetary_penalties_for_breaches_of_financial_sanctions.pdf). For the CMA, see https://www.gov.uk/government/publications/leniency-and-no-action-applications-in-cartel-cases and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf.

55 ICO, Regulatory Action Policy, pp. 24 and 28 (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf). An example of the ICO's tough approach is the £400,000 fine and criminal penalty handed to Keurboom Communications after Keurboom failed to comply with an information notice regarding a breach of the Privacy and Electronic Communication Regulations (ICO Monetary Penalty Notice to Keurboom Communications Ltd (https://ico.org.uk/media/action-weve-taken/enforcement-notices/2014013/mpn-keurboom-ltd-20170503.pdf).

© Law Business Research 2021

certain anti-money laundering failures, for example), and the corporate's level of co-operation will be one factor that authorities usually take into account when deciding what route to pursue.[56]

9.5 Compliance

Enforcement authorities such as the SFO have been focusing increasingly on the compliance programmes of corporates under investigation. For example, the SFO considers the quality of a compliance programme relevant to whether a prosecution is in the public interest, whether the corporate should be invited into DPA negotiations and what the terms of the outcome of those negotiation should include. An organisation's compliance programme is also considered relevant to whether it has an 'adequate procedures' defence to the offence under section 7 of the UK Bribery Act 2010 of failing to prevent bribery or a 'reasonable prevention procedures' defence to the offence of failing to prevent the facilitation of tax evasion under the Criminal Finances Act 2017. It is also relevant to sentencing.[57] Therefore, even if a corporate co-operates with the SFO, its pre-existing compliance programme, any changes it has made to it during the investigation, and the scope for improvement will be relevant considerations as to whether a DPA will be considered appropriate and, if so, on what terms. The ICO has similarly highlighted the importance of adequate compliance programmes.[58] A corporate should therefore expect that in any engagement with the SFO (and probably other prosecuting authorities too), it will need to be prepared to commit significant resources to explaining and enhancing its compliance environment.

See Chapter 46 on compliance

9.6 New management

Recent DPAs have focused on a change in a corporate's cultural framework. This is an important factor when considering whether a DPA is appropriate and features heavily in external communications about DPAs from senior SFO personnel. In practice, this means the SFO will consider whether corporate leadership is the same as at the time of the misconduct and, separately, whether

56 In March 2021, for example, the FCA announced criminal proceedings against NatWest for alleged breaches of regulations 8(1), 8(3) and 14(1) of the Money Laundering Regulations 2007 (MLR 2007). This is a significant landmark, as the FCA's first criminal prosecution under the MLR 2007, indicating a willingness to pursue a criminal outcome in relation to anti-money laundering systems and controls issues (https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc).

57 SFO Operational Handbook, Evaluating a Compliance Programme, p. 1 (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/evaluating-a-compliance-programme/).

58 For the ICO, 'wilful or negligent approach to compliance' is an aggravating factor indicating that more serious regulatory action should be taken (Regulatory Action Policy, p. 11 (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf)).

© Law Business Research 2021

responsible individuals are appropriately held to account. This informs the SFO's degree of confidence that the misconduct will not be repeated.

In the *AFWEL* case, cultural change resulted in a meaningful reduction of the financial penalty and the court stated that the DPA would not have gone ahead if the criminal activity were not so remote from the corporate in its present form.[59] This emphasis on a change in a corporate's culture continues a thread first introduced in the *Sarclad* DPA of 2016.[60]

Companies tend to co-operate for a number of reasons 9.7

With all that said, corporates increasingly choose to co-operate with regulators and enforcement bodies, in many cases very extensively. Sometimes this is just a matter of being a good corporate citizen and maintaining integrity in the eyes of stakeholders, government and the general public. Sometimes there will be considerable stakeholder pressure. Sometimes there is an ongoing relationship with the investigating authority to consider either in the context of previous enforcement proceedings, or where the corporate is in an industry that faces heavy regulatory scrutiny.

In other cases, there may be significant strategic benefits to co-operating. Without some degree of co-operation, a corporate will have little control over, or ability to influence, an investigation. Co-operation that is thorough and genuine may help to resolve the issue in a non-adversarial way (e.g., through a DPA), while retaining some control over what, if any, admissions are made and what is said publicly by the relevant authority.[61]

Few corporates will take lightly the financial implications of a prolonged investigation, or the management time and business interruption it entails. Nor can corporates afford to be dismissive of the effects of a drawn-out process on employee morale and the risk of 'talent flight'. For many companies, gaining

59 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021], para. 29.

60 *SFO v. Sarclad Ltd*, Approved Judgment (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509.

61 A DPA is not, however, guaranteed, even for companies that co-operate. In *R v. Skansen*, a case prosecuted by the CPS in March 2018, the corporate defendant – which was by then dormant – was convicted, following a trial under s.7 UK Bribery Act. The corporate had demonstrated co-operation by having investigated and self-reported conduct to the police that might not otherwise have come to light, and by co-operating with the police and CPS. However, a DPA was not offered. The judge questioned why a prosecution was being brought against a dormant corporate against whom it was agreed that no financial penalty could be imposed and whose only sentence could be an absolute discharge. The status of the corporate, and a desire to send a deterrent message appear to have been the reasons: the CPS said that the public interest test for a prosecution was satisfied so that a message could be sent to others in the industry and they had decided that no ongoing benefit could be achieved by a DPA. The SFO has brokered four DPAs to date, while the CPS has not agreed any. This case is a reminder that a DPA is by no means a predictable outcome – particularly with agencies other than the SFO – even when co-operation exists.

© Law Business Research 2021

clarity and certainty and being able to focus on day-to-day business will be an absolute priority.

Finally, no corporate will relish the prospect of a criminal conviction and the reputational impact this will have. Undoubtedly, the mark of criminal conviction carries a major deterrent, such that an alternative, such as a DPA, is perceived to be a better outcome. For many companies, there may be broader implications of a criminal conviction, such as debarment from public tendering, that outweigh the narrow legal merits of challenging allegations of wrongdoing.

9.8 Multi-agency and cross-border investigations

Corporates should expect the involvement of multiple agencies across multiple jurisdictions as the co-operation between agencies and authorities increases. The ways in which regulators and criminal prosecutors choose to co-operate with each other are many and varied (through informal channels of communication, information gateways, memoranda of understanding and other means).[62] There is undoubtedly an increasing desire for agency co-operation on domestic and international levels and this is being borne out in practice, with co-operation between agencies (both within the United Kingdom and on a multi-jurisdictional basis) becoming increasingly common.[63] Co-operation may be formal or informal, and may range from passive information sharing or more active roles, including interviewing witnesses and allowing secondments.[64]

Voluntary co-operation with an authority can result in requests for the corporate to obtain documents from overseas, wherever possible, as a

62 Authorities commonly enter into memoranda of understanding (MOUs) with authorities in their own or other jurisdictions where both exercise similar functions or are concerned with the same issues. MOU are not legally binding, but declare a shared commitment and aim to provide useful guidelines enabling faster and more efficient sharing of information.

63 The SFO's Airbus investigation, for example, was part of a broader international law enforcement effort that involved France's National Financial Prosecutor's Office and the US Department of Justice (DOJ) and Department of State relating to conduct in several countries, including China, Colombia, Nepal, Russia, South Korea, Saudi Arabia, Taiwan and the United Arab Emirates (*SFO v. Airbus*, Approved Judgment (Case No. U20200108) [2020] 1 WLUK 435, para. 3). In the SFO's investigation into Amec Foster Wheeler, there was co-operation between the SFO, the US Securities and Exchange Commission and the DOJ, and Brazil's Federal Comptroller General, Attorney General of the Union and Federal Public Ministry relating to conduct in several countries, including Malaysia, Nigeria, Saudi Arabia, India and Brazil (*Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021]).

64 For example, in December 2016 the US DOJ Criminal Division announced it would second a lawyer to the United Kingdom to work at the FCA and the SFO to further co-operation between the jurisdictions and share best practice (https://www.sfo.gov.uk/2016/12/09/us-department-justice-secondee/).

© Law Business Research 2021

demonstration of its ongoing and genuine co-operation.[65] A corporate will need to consider all relevant data privacy laws when considering whether to comply with these requests voluntarily.

Strategies for dealing with multiple authorities 9.9

Corporates should proceed on the assumption that authorities share, or will share, information and materials, and are likely to obtain evidence from multiple sources, not just from the corporate itself. Accordingly, a coherent strategy should be formulated from the outset. The corporate may find it sensible to engage in an open and pragmatic dialogue with each authority and be proactive in encouraging the authorities to take the same approach with each other wherever possible. Ultimately, if more than one agency has a legitimate basis on which to enforce, it is usually preferable to bring the matter to a combined resolution.

The SFO has set out the factors its prosecutors should consider when assessing whether to enter into a DPA if there is a parallel investigation by another agency in the United Kingdom or overseas, which include the need for early communication and harmonising the approach to matters such as witnesses and privilege, ensuring consistent positions on facts and liability, and coordinating on practical issues such as court dates and market announcements.[66]

There are also additional points for corporates to consider when dealing with multi-agency investigations, including:

- considering what enquiries or internal investigation should be conducted;
- considering which authorities are likely to be more influential or proactive;
- ensuring that a consistent approach is taken to explanations, documents and privilege; and
- if entering settlement discussions, considering whether it would be beneficial or possible to engage with all authorities at the same time.

Conclusion 9.10

Corporates are increasingly expected to co-operate with regulatory agencies and criminal authorities fulsomely, even when their co-operation is voluntary. The DPAs that corporates have entered into with the SFO demonstrate this expectation, but this behaviour is increasingly expected from regulators and enforcement bodies across the spectrum.

65 Where a corporate does not voluntarily provide such documents, the SFO may seek to compel production. The High Court of England and Wales ruled in *R (KBR Inc.) v. SFO* [2018] EWHC 2012 (Admin) that the scope of the SFO's power to compel the production of data extends to data of a UK corporate held abroad and data of a non-UK corporate held abroad, provided there is a 'sufficient connection' between that corporate and the United Kingdom.

66 SFO Operational Handbook, Deferred Prosecution Agreements (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/).

© Law Business Research 2021

There is increasing pressure on corporates from the public, stakeholders and government to act as good corporate citizens. Maintaining credibility with capital markets can be an additional factor in a decision to co-operate.

Co-operation is relevant at every stage of an investigation, and for every outcome. It requires significant commitment: continual and genuine assistance, prompt self-reporting, and access to hard copy materials, electronic data and potential witnesses. Multiple agencies may also be involved, with differing requests. There can be many benefits to co-operating fulsomely, but it is no easy task.

© Law Business Research 2021

10

Co-operating with the Authorities: The US Perspective

John D Buretta, Megan Y Lew and Jingxi Zhai[1]

Government investigations of corporations can start quietly or loudly. A subpoena might arrive in the mail; an employee might speak up to a manager; federal agents might raid the offices and seize files, computers and cell phones; or border patrol agents might stop an employee, or a CEO, at the airport. However an investigation commences, a critical question at the outset is whether the company should co-operate in a government inquiry, and, if so, how, and to what extent. Like a game of chess, a company's opening moves can dictate the end game and must be chosen with care. In the best case, investigations quickly and cost-effectively point the authorities toward individual wrongdoers, the company's effort is short-lived, and it incurs no penalty. In the worst case, Pandora's box is opened.

While the decision to co-operate will turn on the unique factual and legal circumstances faced by a company, this chapter aims to guide the reader through the decision-making process, whether the investigation concerns the Foreign Corrupt Practices Act (FCPA), securities, antitrust or sanctions laws, or the False Claims Act, or other government actions. This chapter discusses how US government authorities define co-operation, identifies the pros and cons of co-operating with the authorities and highlights special considerations in multi-agency and cross-border investigations.

What is co-operation? 10.1

Co-operating with a US government authority generally entails providing all relevant, non-privileged information. This can amount to ensuring that key

1 John D Buretta is a partner, Megan Y Lew is a practice area attorney and Jingxi Zhai is an associate at Cravath, Swaine & Moore LLP.

© Law Business Research 2021

witnesses are available for interviews by the government, sharing information gleaned from internal interviews of employees, providing relevant documents as well as context and background for those documents, giving factual presentations, and agreeing to take remedial action where appropriate.

10.1.1 Department of Justice's general approach to co-operation

The Department of Justice (DOJ) issues guidance and policies for prosecutors in its Justice Manual. Its chapter on Principles of Federal Prosecution of Business Organizations sets forth ten factors that prosecutors should consider when investigating, deciding whether to charge and negotiating a plea or other agreement with a company. Among these is consideration for 'the corporation's willingness to cooperate, including as to potential wrongdoing by its agents'.[2] The Justice Manual states that a company is eligible for co-operation credit if it:

> *identif[ies] all individuals substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide[s] to the Department all relevant facts relating to that misconduct. If a company seeking co-operation credit declines to learn of such facts or to provide the Department with complete factual information about the individuals substantially involved in or responsible for the misconduct, its co-operation will not be considered a mitigating factor under this section.*[3]

In other words, to obtain co-operation credit, a company must provide all non-privileged facts concerning misconduct.[4] In addition, the company must not intentionally remain ignorant about misconduct and cannot cherry-pick facts to share with the DOJ.[5]

The DOJ's current approach to co-operation, as reflected in the Justice Manual, emphasises holding individuals accountable for their misconduct and requires companies to disclose the identities of all individuals involved. The DOJ's approach to co-operation has evolved over the years, often changing

2 US Dep't of Justice (DOJ), Justice Manual § 9-28.300. Additional noteworthy factors include 'the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision' and 'the corporation's remedial actions, including, but not limited to, any efforts to implement an adequate and effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, or to pay restitution'. Id. In June 2020, the DOJ released an updated guidance document concerning these factors, entitled Evaluation of Corporate Compliance Programs, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

3 DOJ, Justice Manual §§ 9-28.300, 9-28.700.

4 Id. § 9-28.720.

5 Id. § 9-28.700 ('If a company seeking cooperation credit declines to learn of such facts or to provide the Department with complete factual information . . . its cooperation will not be considered a mitigating factor under this section.').

© Law Business Research 2021

with each new administration, as articulated through a series of DOJ policy speeches. Prior to September 2015, companies might obtain partial co-operation credit without identifying the individual wrongdoers to the DOJ; this might even have been sufficient to avoid charges in some instances.[6] In September 2015, in the so-called 'Yates Memo', the DOJ announced that co-operation would require disclosure of *all* individual misconduct, regardless of the individual's title or seniority at the company.[7] In November 2018, the DOJ scaled back this requirement for co-operation credit, announcing a policy revision that required companies to identify only individuals substantially involved in or responsible for misconduct.[8] Most recently, in October 2021, the DOJ rescinded its prior 2018 guidance, stating that it will 'no longer be sufficient for companies to limit disclosures to those they assess to be "substantially involved" in the misconduct'.[9] Instead, the DOJ returned to its guidance under the Yates Memo, requiring identification of *all* individuals involved and *all* non-privileged information about individual wrongdoing for companies to be eligible for co-operation credit.[10] This change in guidance makes it more difficult to obtain co-operation credit because companies must provide significant detail about all employees and management involved in the alleged misconduct. The DOJ's evolving approach continues to reflect the inherent challenges in charging individuals in complex, white-collar investigations, where prosecutors often must sort through and understand 'complex corporate hierarchies [and] enormous volumes of electronic documents' while navigating 'a variety of legal and practical challenges that can limit access to the evidence' that the DOJ needs to bring charges against individuals, especially when evidence is located outside the United States.[11]

What does this mean in practice for a company under investigation? The DOJ wants to learn information such as: how and when the alleged misconduct

6 Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (10 September 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

7 Id.

8 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

9 Lisa O Monaco, Deputy Att'y Gen., DOJ, Keynote Address at the American Bar Association's 36th National Institute on White Collar Crime (28 October 2021), available at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

10 Id.

11 Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (10 September 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

© Law Business Research 2021

occurred; who promoted or approved it; who was responsible for committing it;[12] and all individuals involved in setting a company on a course of criminal conduct, regardless of their position, status or seniority.[13] To provide this, company counsel may relay facts to the DOJ by producing relevant documents, allowing the DOJ to interview employees (including acquiescing to 'deconfliction' requests from the DOJ that the government interview employees before company counsel does so), proffering information obtained from an internal investigation or analysing voluminous or complex documents. To obtain full credit, the DOJ will consider the timeliness of the disclosures, whether the company undertook a proactive approach to co-operating, and the thoroughness of the company's investigation.[14] The DOJ does not expect companies to undertake a 'years-long, multimillion dollar investigation every time a company learns of misconduct'; rather, companies are expected 'to carry out a thorough investigation tailored to the scope of the wrongdoing'.[15] The DOJ, consistent with indications from Attorney General Merrick Garland, said that its 'first priority in corporate criminal matters [is] to prosecute the individuals who commit and profit from corporate malfeasance'.[16] In practice, companies seeking co-operation therefore need not 'have all the facts lined up on the first day' they talk to the DOJ, but they should turn over relevant information to the DOJ on a rolling basis as they receive it.[17]

To ensure that the company's disclosures to the DOJ are extensive and that its internal investigation is thorough, and to fulfil the DOJ's own obligation to make just decisions based on the fullest possible set of facts, the DOJ usually undertakes its own parallel investigation. Accordingly, the Justice Manual instructs prosecutors to:

> *proactively investigat[e] individuals at every step of the process – before, during, and after any corporate co-operation. Department attorneys should vigorously review any information provided by companies and compare it to*

12 DOJ, Justice Manual § 9-28.720.

13 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0; Lisa O Monaco, Deputy Att'y Gen., DOJ, Keynote Address at the American Bar Association's 36th National Institute on White Collar Crime (see supra note 9).

14 DOJ, Justice Manual § 9-28.700.

15 Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at the New York City Bar Association White Collar Crime Conference (10 May 2016), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-new-york-city-bar-association.

16 Lisa O Monaco, Deputy Att'y Gen., DOJ, Keynote Address at the American Bar Association's 36th National Institute on White Collar Crime (see supra note 9).

17 Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at the New York City Bar Association White Collar Crime Conference (see supra note 15).

© Law Business Research 2021

> *the results of their own investigation, in order to best ensure that the information provided is indeed complete and does not seek to minimize, exaggerate, or otherwise misrepresent the behaviour or role of any individual or group of individuals.*[18]

Counsel may encounter situations where it is unclear whether misconduct has actually occurred, because the corporate client either does not have access to the relevant information or, even with full access, cannot discern whether there is malfeasance. In this regard, the DOJ has emphasised that it 'just want[s] the facts' – it does not expect counsel for the company 'to make a legal conclusion about whether an employee is culpable, civilly or criminally'.[19]

In other cases, a company may find that relevant documents in a foreign location cannot be produced to US authorities because of foreign data privacy, bank secrecy or other blocking laws. The Justice Manual recognises that such situations may occur and acknowledges that a company may still be eligible for co-operation credit, though the company will bear the burden of explaining why co-operation credit is still justified despite the restrictions faced by the company in gathering or disclosing certain facts.[20]

The DOJ has emphasised that co-operation does not require a company to waive the attorney–client privilege or the attorney work-product protection.[21] While a company may decide to waive these privileges and protections when it suits its interests to do so, prosecutors may not request such a waiver.[22]

Other Department of Justice policies regarding co-operation 10.1.2

Several components of the DOJ maintain policies regarding company co-operation separate from the guidelines set out in the Justice Manual. Three examples are discussed below: (1) the Criminal Division's policy regarding FCPA enforcement, (2) the Antitrust Division's leniency programme and (3) the Civil Division's False Claims Act enforcement policy.

The FCPA Pilot Program and Corporate Enforcement Policy 10.1.2.1

In April 2016, the DOJ announced a pilot programme for FCPA cases with the goal of motivating 'companies to voluntarily self-disclose FCPA-related misconduct, fully cooperate with the [DOJ Criminal Division's] Fraud Section, and,

18 DOJ, Justice Manual § 9-28.700.

19 Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at the New York City Bar Association White Collar Crime Conference (see supra note 15).

20 DOJ, Justice Manual § 9-28.700.

21 Id. § 9-28.710.

22 Id. See also Memorandum from Mark Filip, Deputy Att'y Gen., DOJ, to Heads of Department Components and United States Attorneys (28 August 2008), available at https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

© Law Business Research 2021

where appropriate, remediate flaws in their controls and compliance programs'.[23] The Pilot Program, which was initially meant to last one year, became a permanent DOJ programme in November 2017.[24] Known as the FCPA Corporate Enforcement Policy, it is designed to encourage companies to self-report any potential FCPA violations and promote increased co-operation with the DOJ.[25]

To be eligible for the full benefits of the FCPA Corporate Enforcement Policy, companies must: (1) voluntarily self-report all facts within a reasonably prompt time, (2) offer full co-operation and (3) undertake remedial measures in a timely fashion.[26] In addition, the company must disgorge all profits related to the misconduct.[27] If a company complies with these requirements, the DOJ will apply a presumption that the matter will be resolved through a declination.[28] If aggravating circumstances lead the DOJ to determine that declination is not appropriate, the DOJ will nonetheless recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines' fine range for the offence and will generally not require appointment of a monitor.[29] As of November 2021, the DOJ has issued 14 declination letters under the FCPA Corporate Enforcement Policy.[30]

'Th[e] presumption [of declination] may be overcome only if there are aggravating circumstances related to the nature and seriousness of the offense, or if the offender is a criminal recidivist.'[31] For example, in June 2020, the DOJ reached a US$233 million settlement agreement with Novartis AG, Alcon Inc (a former Novartis subsidiary) and their subsidiaries over violations of the FCPA. Novartis admitted that it conspired to violate the FCPA by bribing employees of state-owned and state-controlled hospitals in Greece to increase the sales of Novartis pharmaceutical products, among other violative conduct. Notably, Alcon's monetary penalty reflected a 25 per cent reduction off the

23 Leslie R Caldwell, Ass't Att'y Gen., DOJ, Criminal Division Launches New FCPA Pilot Program (5 April 2016), available at https://www.justice.gov/archives/opa/blog/criminal-division-launches-new-fcpa-pilot-program.

24 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (29 November 2017), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign.

25 Id.

26 FCPA Corporate Enforcement Policy, DOJ, Justice Manual § 9-47.120.

27 Id.

28 Id; Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (see supra note 24).

29 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (see supra note 24); FCPA Corporate Enforcement Policy, DOJ, Justice Manual § 9-47.120.

30 DOJ, Declinations (2 September 2021), available at https://www.justice.gov/criminal-fraud/corporate-enforcement-policy/declinations.

31 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (see supra note 24).

© Law Business Research 2021

bottom of the applicable US Sentencing Guidelines' range due to its 'full cooperation with the government's investigation'. On the other hand, Novartis received only a 25 per cent reduction from the approximate midpoint of the Guidelines' range despite fully co-operating and engaging in remediation because of recidivism – 'its parent company . . . was involved in similar conduct for which it previously reached a resolution with the SEC in March 2016'.[32]

In November 2019, the DOJ made clarifying revisions to certain provisions of the FCPA Corporate Enforcement Policy. First, the DOJ changed a policy that stated a company must alert the DOJ when it 'is or should be aware of opportunities' to 'obtain relevant evidence not in the company's possession and not otherwise known to the Department'. The change removed the words 'or should be' leaving only 'is aware', so that the company must now only report opportunities to obtain evidence not in its possession when it is actually aware of such evidence. Second, the November 2019 update makes clear that self-disclosure following only a preliminary investigation is acceptable and may earn self-disclosure credit. A footnote in the self-disclosure section now underscores that a company 'may not be in a position to know all relevant facts at the time of a voluntary self-disclosure, especially where only preliminary investigative efforts have been possible' and instructs companies to make clear during a self-disclosure whether their knowledge is based on a preliminary investigation. Third, as later stated in October 2021, the DOJ reinstated its 2015 guidance that companies must turn over relevant facts related to 'all individuals' who played a part in a 'violation of law'.[33] This 2021 guidance rescinded the previous version of the policy, which stated that to receive self-disclosure credit, companies must turn over all relevant facts related to 'any individuals' who played a substantial part in the 'misconduct at issue'.[34]

In January 2020, the DOJ secured the largest global foreign bribery resolution to date, in which co-operation credit played a significant role. Specifically, the DOJ entered into a deferred prosecution agreement (DPA) with Airbus SE, whereby the company agreed to pay over US$3.9 billion in total to several

32 DOJ, press release, 'Novartis Hellas S.A.C.I. and Alcon Pte Ltd Agree to Pay Over $233 Million Combined to Resolve Criminal FCPA Cases', (25 June 2020), available at https://www.justice.gov/opa/pr/novartis-hellas-saci-and-alcon-pte-ltd-agree-pay-over-233-million-combined-resolve-criminal.

33 Lisa O Monaco, Deputy Att'y Gen., DOJ, Keynote Address at the American Bar Association's 36th National Institute on White Collar Crime (see supra note 9); Sally Quillian Yates, Deputy Att'y Gen., DOJ, Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (10 September 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

34 Judy Godoy, 'DOJ Tweaks FCPA Corporate Enforcement Policy for Clarity', *Law360* (20 November 2019), available at https://www.law360.com/securities/articles/1221939/doj-tweaks-fcpa-corporate-enforcement-policy-for-clarity; FCPA Corporate Enforcement Policy, DOJ, Justice Manual § 9-47.120.

© Law Business Research 2021

government authorities in and outside the United States, in part to resolve foreign bribery charges brought under the FCPA. The FCPA charges were predicated on Airbus' scheme to bribe foreign officials to obtain and retain business, namely contracts to sell aircraft. Notably, the DOJ stated that the resolution 'reflects the significant benefits available . . . for companies that choose to self-report export violations, cooperate, and remediate as to those violations, even where there are aggravating circumstances'. Airbus also agreed in the DPA to 'continue to cooperate with the department in any ongoing investigations and prosecutions relating to the conduct'.[35]

10.1.2.2 The antitrust leniency programme

The DOJ Antitrust Division has a corporate leniency programme granting leniency to the first company that (1) self-discloses conduct related to unlawful anti-competitive conspiracies and (2) co-operates with the DOJ's ensuing investigation.[36] A company that has been granted leniency is only liable for the actual damages in related follow-on litigation, rather than treble damages.[37] Additionally, a company given leniency is not liable for the damages caused by other members of the conspiracy, which a conspirator typically would be responsible for under a theory of joint-and-several liability in antitrust conspiracy cases.[38]

The Antitrust Division expects companies that receive leniency to provide 'truthful, continuing, and complete cooperation', which includes 'conducting a timely and thorough internal investigation, providing detailed proffers of the reported conduct, producing documents no matter where they are located, and making cooperative witnesses available for interviews'.[39]

While only the first company to self-report and co-operate can receive leniency, subsequent co-operators may still be rewarded for their efforts. The Antitrust Division recently clarified that the extent of any fine reduction does not merely reflect the timing of co-operation, but will also reflect the 'nature, extent, and value of that cooperation to the investigation'.[40] Nevertheless, the

35 DOJ, 'Airbus Agrees to Pay Over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case', press release (31 January 2020), available at https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

36 DOJ, Frequently Asked Questions About the Antitrust Division's Leniency Program and Model Leniency Letters (26 January 2017), available at https://www.justice.gov/atr/page/file/926521/download.

37 Id.; Antitrust Criminal Penalty Enhancement and Reform Act of 2004 § 213(a).

38 DOJ, Frequently Asked Questions About the Antitrust Division's Leniency Program and Model Leniency Letters (26 January 2017), available at https://www.justice.gov/atr/page/file/926521/download; Antitrust Criminal Penalty Enhancement and Reform Act of 2004 § 213(a).

39 Richard A Powers, Deputy Assistant Att'y Gen., DOJ, Remarks at the 13th International Cartel Workshop (19 February 2020), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-powers-delivers-remarks-13th-international.

40 Id.

© Law Business Research 2021

Division maintains that 'the earlier the cooperation is provided, the more valuable it usually is in assisting the [D]ivision's efforts'.[41] If a company's cooperation is insufficient, the Division 'will not hesitate' to withhold a fine reduction and may even increase the fine.[42]

Traditionally, the Antitrust Division did not use DPAs to resolve criminal antitrust matters since, under the leniency programme, companies that were the first to self-report and co-operate could be fully insulated from prosecution.[43] However, in 2019, it announced that DPAs could be an option for companies that did not obtain leniency but had an effective compliance programme.[44] Since then, as of July 2021, it has entered into nine DPAs.[45] Despite this development, the Antitrust Division continues to expect that companies will seek leniency as the benefits under the leniency programme are more generous than those associated with a DPA.[46]

The False Claims Act 10.1.2.3

In May 2019, for the first time, the DOJ issued guidelines for awarding entities with co-operation credit in False Claims Act (FCA) cases.[47] The FCA, frequently used in healthcare litigation, imposes civil liability on entities that defraud government programmes.[48] While the new federal guidance does not present any radically new considerations, it does provide helpful standards and brings FCA cases in line with existing DOJ practices in other types of investigations.[49]

The federal guidance contemplates three main factors that the DOJ will consider in determining eligibility for and the extent of co-operation credit in FCA matters. First, the DOJ weighs whether eligibility should be available for voluntary self-disclosure by entities that discover conduct that violates the

41 Id.

42 Id.

43 Id.

44 Id.

45 Justin Murphy, Brian Boyle and Alexandra Lewis, 'A Potential Shift in Antitrust Deferred Prosecution Agreements', *Law360* (30 July 2021), available at https://www.law360.com/articles/1405408/a-potential-shift-in-antitrust-deferred-prosecution-agreements.

46 Richard A Powers, Deputy Assistant Att'y Gen., DOJ, Remarks at the 13th International Cartel Workshop (see supra note 39).

47 DOJ, Department of Justice Issues Guidance on False Claims Act Matters and Updates Justice Manual (7 May 2019), available at https://www.justice.gov/opa/pr/department-justice-issues-guidance-false-claims-act-matters-and-updates-justice-manual.

48 False Claims Act, 31 U.S.C. §§ 3729–3733 (2012).

49 Peter B Hutt II, Michael Wagner, Michael Maya and Brooke Stanley, 'New DOJ Cooperation Credit Guidelines a Welcome Sign, but Key Questions Remain Unresolved', Inside Government Contracts (9 May 2019), available at https://www.insidegovernmentcontracts.com/2019/05/new-doj-cooperation-credit-guidelines-a-welcome-sign-but-key-questions-remain-unresolved/.

© Law Business Research 2021

FCA.[50] Notably, co-operation credit is not limited to entities that self-disclose before an investigation commences. Rather, if '[d]uring the course of an internal investigation into the government's concerns . . . entities . . . discover additional misconduct going beyond the scope of the known concerns, . . . the voluntary self-disclosure of such additional misconduct will qualify the entity for credit'.[51] Second, the DOJ considers whether the entity has provided assistance to an ongoing government investigation, including, but not limited to, identifying employees or individuals responsible for the misconduct, accepting responsibility for the misconduct, making employees available for depositions and interviews, and preserving and collecting relevant information and data in excess of what is required by law.[52] Finally, the DOJ considers the extent to which entities have undertaken remedial measures in response to an FCA violation.[53]

In January 2020, the DOJ announced a new reform to the policy. To complement the existing incentives to voluntarily disclose and co-operate, the Department will now also consider the 'nature and effectiveness of a company's compliance system' in determining whether prosecution under the FCA is the appropriate remedy.[54] This reform in part reflects that a key element of the FCA is the scienter requirement 'and a robust compliance program executed in good faith could demonstrate the lack of scienter'.[55] The DOJ also emphasised that 'good corporate citizens that effectively police themselves should not be subjected to unnecessary enforcement costs'.[56]

See Chapter 46 on compliance

10.1.3 Approaches to co-operation by other federal agencies

Other US enforcement agencies take similar approaches to rewarding company co-operation. Two examples of such agency processes – the US Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) – are described below.

The SEC's approach to co-operation was first described in a report of investigation and statement regarding the public company Seaboard.[57] This report, which became known as the 'Seaboard Report', concluded that charges

50 DOJ, Justice Manual § 4-4.112.

51 Id.

52 Id.

53 Id.

54 Stephen Cox, Deputy Associate Att'y Gen., DOJ, Keynote Remarks at the 2020 Advanced Forum on False Claims and Qui Tam Enforcement (27 January 2020), available at https://www.justice.gov/opa/speech/deputy-associate-attorney-general-stephen-cox-provides-keynote-remarks-2020-advanced.

55 Id.

56 Id.

57 US Securities and Exchange Commission (SEC), Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Co-operation to Agency Enforcement Decisions, Release No. 34-44969

© Law Business Research 2021

against Seaboard were not warranted based on the consideration of four broad factors: (1) self-policing by the company prior to the discovery of the misconduct; (2) self-reporting the misconduct to the SEC, including investigating the misconduct; (3) remediation of the misconduct; and (4) co-operation with the SEC.[58] The benefits of co-operating with the SEC could range from the SEC 'declining an enforcement action, to narrowing charges, limiting sanctions, or including mitigating or similar language in charging documents'.[59] Entry into a deferred or non-prosecution agreement may also be an option depending on the level of co-operation from the company.[60] Similar to the DOJ's current approach, the SEC expects a co-operating company to provide 'the Commission staff with all information relevant to the underlying violations and the company's remedial efforts'.[61]

The CFTC, which regulates US derivatives markets, also offers co-operation credit. While the CFTC has had a long-standing policy of offering co-operation credit, in 2017 it issued advisories that further incentivised 'individuals and companies to cooperate fully and truthfully in CFTC investigations and enforcement actions'.[62] Similar to the approaches adopted by the DOJ and SEC, the CFTC will, in its discretion, consider the following broad factors in determining whether to grant co-operation credit: (1) 'the value of the co-operation' to the instant investigation and enforcement action; (2) 'the value of the co-operation to the [CFTC's] broader law enforcement interests';

(23 October 2001) (Seaboard Report), available at https://www.sec.gov/litigation/investreport/34-44969.htm.

58 Id. See also SEC, Spotlight on Enforcement Cooperation Program (20 September 2016), available at https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml.

59 Andrew Ceresney, Director, SEC Division of Enforcement, 'The SEC's Co-operation Program: Reflections on Five Years of Experience', Remarks at University of Texas School of Law's Government Enforcement Institute in Dallas, Texas (13 May 2015), available at https://www.sec.gov/news/speech/sec-cooperation-program.html.

60 Id. See, e.g., SEC, Deferred Prosecution Agreement between Tenaris, S.A. and the SEC (23 March 2011), available at https://www.sec.gov/news/press/2011/2011-112-dpa.pdf; SEC, Akamai Technologies, Inc. Non-Prosecution Agreement (3 May 2016), available at https://www.sec.gov/news/press/2016/2016-109-npa-akamai.pdf.

61 SEC, Spotlight on Enforcement Cooperation Program (20 September 2016), available at https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml.

62 US Commodity Futures Trading Commission (CFTC), CFTC's Enforcement Division Issues New Advisories on Co-operation, Release Number 7518-17 (19 January 2017), available at https://cftc.gov/PressRoom/PressReleases/7518-17. See CFTC, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf; CFTC, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Individuals (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryindividuals011917.pdf.

© Law Business Research 2021

(3) 'the culpability of the company or individual and other relevant factors'; and (4) 'uncooperative conduct that offsets or limits credit that the company or individual would otherwise receive'.[63] The CFTC's advisories emphasise that co-operation credit will be given to co-operation that is 'sincere', 'robust' and 'indicative of a willingness to accept responsibility for the misconduct'.[64] The benefits of co-operating with the CFTC range from the agency taking no enforcement action to imposing reduced charges against the co-operating company.[65] Furthermore, in March 2019, the CFTC announced a new advisory on self-reporting and co-operation to build on the existing foundation of co-operation to further incentivise 'individuals and companies to self-report misconduct, cooperate fully in CFTC investigations and enforcement actions, and appropriately remediate to ensure the wrongdoing does not happen again'.[66]

The CFTC advisories collectively list dozens of specific and concrete factors that the agency will consider when assessing whether to grant co-operation credit.[67] Company counsel may find it beneficial to refer to these factors when determining the company's course of action at various points in time, such as when learning about misconduct, investigating misconduct, self-disclosing misconduct to government authorities and co-operating with government authorities. For example, the advisory concerning co-operation by companies includes a section concerning the 'quality' of the company's co-operation, which the advisory states should be assessed by looking at whether the company 'willingly used all available means to . . . preserve relevant information', 'make employee testimony' or company documents 'available in a timely manner', 'explain transactions and interpret key information' and 'respond quickly to requests and subpoenas for information' from the CFTC, among other things.[68] Indeed, these considerations are relevant to any situation where a company is considering co-operating with authorities, regardless of the type of misconduct or whether the misconduct falls under the jurisdiction of the CFTC.

10.1.4 Case studies: Walmart and Goldman Sachs

Choosing to co-operate with the government is not a one-size-fits-all decision, and companies sometimes choose to (or may be able to) co-operate with some

63 CFTC, CFTC's Enforcement Division Issues New Advisories on Co-operation, Release No. 7518-17 (19 January 2017), available at https://cftc.gov/PressRoom/PressReleases/7518-17.

64 CFTC, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (see supra note 62).

65 Id.

66 CFTC, CFTC Division of Enforcement Issues Advisory on Violations of the Commodity Exchange Act Involving Foreign Corrupt Practices, Release No. 7884-19 (6 March 2019), available at https://www.cftc.gov/PressRoom/PressReleases/7884-19.

67 See CFTC, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (see supra note 62).

68 Id.

© Law Business Research 2021

aspects of a government investigation, but not others. Two examples of settlements of criminal charges brought by the DOJ for FCPA violations, involving Walmart Inc and the Goldman Sachs Group Inc, are described below.

In June 2019, Walmart and a Brazilian Walmart subsidiary agreed to pay US$137 million to settle criminal charges brought by the DOJ in connection with FCPA violations. These allegations arose out of conduct that occurred from 2000 to 2011, in which Walmart employees failed to implement and maintain the company's internal accounting controls to prevent improper payments to foreign government officials. Crucially, certain senior executives at the company were aware of this lapse in controls, yet these practices persisted.[69]

Walmart's co-operation with the government led to a reduction in the overall fine that was levied against the company. Walmart fully co-operated with the investigations into conduct in Brazil, China and India; however, it did not provide full documents and information in connection with the Mexican investigation and chose to interview a key witness before making the witness available for a DOJ interview, contrary to the DOJ's request. Furthermore, Walmart did not self-disclose the misconduct that occurred in Mexico, though it did disclose the conduct in the other countries after the government began investigating the Mexican conduct. Because Walmart fully co-operated with the investigations in Brazil, China and India, it received a 25 per cent reduction in the fines applicable to those jurisdictions under the US Sentencing Guidelines, while it only received a 20 per cent reduction in the fines applicable to the Mexican misconduct.[70]

In October 2020, Goldman Sachs and its Malaysian subsidiary agreed to pay US$2.9 billion to resolve criminal charges brought by the DOJ in connection with certain FCPA violations.[71] These charges arose out of a five-year scheme, from 2009 to 2014, to pay more than US$1.6 billion in bribes to officials in Malaysia and Abu Dhabi to obtain business for Goldman Sachs from 1MDB, a Malaysian state-owned and state-controlled fund created to pursue investment and development projects for the economic benefit of Malaysia and its people. Through this bribery scheme, Goldman Sachs secured lucrative business opportunities, which included, among other things, its role as underwriter on bond deals with a total value of US$6.5 billion. In resolving the charges, Goldman Sachs admitted to conspiring to violate the FCPA in connection with the scheme and, among other admissions, admitted that there were significant red flags raised during the due diligence process that allowed

69 DOJ, 'Walmart Inc. and Brazil-Based Subsidiary Agree to Pay $137 Million to Resolve Foreign Corrupt Practices Act Case', press release (20 June 2019), available at https://www.justice.gov/opa/pr/walmart-inc-and-brazil-based-subsidiary-agree-pay-137-million-resolve-foreign-corrupt.

70 Id.

71 DOJ, 'Goldman Sachs Charged in Foreign Bribery Case and Agrees to Pay Over $2.9 Billion', press release (22 October 2020), available at https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.

© Law Business Research 2021

certain employees to advance the bribery scheme and to divert and misappropriate funds from the bond offerings underwritten by Goldman Sachs. The bank's Malaysian subsidiary pleaded guilty to 'knowingly and willfully' conspiring to violate the FCPA, while Goldman Sachs entered into a DPA with the DOJ.[72]

Goldman Sachs received partial credit for its co-operation with the government, which resulted in a 10 per cent reduction in the overall fine.[73] It did not receive full credit because it allegedly failed to voluntarily disclose the misconduct and significantly delayed producing relevant evidence, such as recorded telephone calls between Goldman Sachs' business and control function personnel about the bribery scheme. The DOJ also credited Goldman Sachs with US$1.6 billion in payments in separate parallel resolutions in the United Kingdom, Singapore and Malaysia.[74]

10.2 Key benefits and drawbacks to co-operation

Deciding whether to co-operate with a government investigation requires careful consideration of the associated benefits and drawbacks. On the one hand, co-operation affords the opportunity of substantially reduced or even no criminal charges and penalties; on the other hand, co-operation brings with it significant risks and costs.

10.2.1 Reduced or no charges and penalties

By and large, companies and individuals choose to co-operate with the government to receive some leniency in the form of reduced (or even no) penalties or charges. Unsurprisingly, research has shown that companies that choose to co-operate with the government tend to achieve better outcomes and typically end up paying lower fines than those that do not.[75] For example, in 2016, Dutch telecommunications company VimpelCom (now known as VEON) paid a criminal fine to the DOJ and Dutch authorities of US$460 million rather than US$836 million to US$1.67 billion, as suggested by the US Sentencing Guidelines, because of the Dutch telecommunications company's co-operation with the DOJ in its investigation of alleged FCPA violations.[76] Similarly, in 2021, British engineering company Amec Foster Wheeler Energy Limited paid US$18.4 million in criminal fines to the DOJ, UK and Brazilian authorities, reflecting a 25 per cent reduction off the applicable US Sentencing

72 Id.

73 Id.

74 Id.

75 See, e.g., Alan Crawford, 'Research Shows It Pays To Cooperate With Financial Investigations', Impact (June 2014), available at http://pac.org/wp-content/uploads/Impact_06_2014.pdf.

76 DOJ, 'VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme', press release (18 February 2016), available at https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million.

© Law Business Research 2021

Guidelines fine for the company's full co-operation and remediation.[77] On the other hand, in 2015, Alstom SA was required to pay a criminal fine of US$772 million, the largest-ever recorded fine for an FCPA violation at that time, in part because of 'Alstom's failure to voluntarily disclose the misconduct . . . [and] Alstom's refusal to fully cooperate with the department's investigation for several years'.[78] More recently, in 2020, Beam Suntory Inc (Beam) was required to pay a criminal fine of US$19 million – a 10 per cent reduction off the applicable US Sentencing Guidelines fine for the company's partial co-operation and remediation – to resolve DOJ charges of FCPA violations. The DOJ awarded only partial credit for cooperation and remediation and no credit for self-disclosure because of Beam's 'failure to fully cooperate', 'significant delays caused by Beam in reaching a timely resolution', 'its refusal to accept responsibility for several years' and Beam's 'failure to fully remediate, including its failure to discipline certain individuals involved in the conduct'. The DOJ also did not credit any of the US$8 million that the company paid to settle parallel charges with the SEC because Beam 'did not seek to coordinate a parallel resolution' with the DOJ.[79]

In addition to the reduced monetary fines that can result from co-operation, the form of a penalty may also vary depending on whether, and how much, a company co-operates with government authorities. If a company has fully co-operated, and if the facts and circumstances warrant such a resolution, the government may consider offering a declination (whereby the government declines to prosecute the entity for any alleged wrongdoing). If a declination is not an option, the next best scenario is a non-prosecution agreement (NPA), which is a contractual agreement between the wrongdoer and the government in which the government agrees not to bring criminal charges in exchange for certain requirements from the company (e.g., a fine, admitting to certain facts, further co-operating with the government or entering into compliance or remediation efforts). Another option in the government's toolbox is a DPA, which is an agreement with the government where criminal charges are filed with the court but prosecution is postponed for a certain period in exchange for the company undertaking certain conditions (e.g., payment of

77 DOJ, 'Amec Foster Wheeler Energy Limited Resolves Foreign Bribery Case and Agrees to Pay Penalty of Over $18 Million', press release (25 June 2021), available at https://www.justice.gov/usao-edny/pr/amec-foster-wheeler-energy-limited-resolves-foreign-bribery-case-and-agrees-pay-penalty.

78 DOJ, 'Alstom Sentenced to Pay $772 Million Criminal Fine to Resolve Foreign Bribery Charges', press release (13 November 2015), available at https://www.justice.gov/opa/pr/alstom-sentenced-pay-772-million-criminal-fine-resolve-foreign-bribery-charges#:~:text=Alstom%20S.A.%2C%20a%20French%20power,%2C%20including%20Indonesia%2C%20Saudi%20Arabia%2C.

79 DOJ, 'Beam Suntory Inc. Agrees to Pay Over $19 Million to Resolve Criminal Foreign Bribery Case', press release (27 October 2020), available at https://www.justice.gov/opa/pr/beam-suntory-inc-agrees-pay-over-19-million-resolve-criminal-foreign-bribery-case.

© Law Business Research 2021

fines, compliance reforms, further co-operating with the government, annual reporting or certification requirements, or the appointment of a monitor). If the company complies with these conditions, the government will move to dismiss the charges at the end of the term of deferment. For example, in April 2020, the DOJ explained that it had, at least in part, agreed to enter into a DPA with the Industrial Bank of Korea to resolve violations of the Bank Secrecy Act because the bank accepted and acknowledged responsibility for its conduct, had conducted a 'thorough internal investigation', provided 'frequent and regular updates' and made non-US-based employees available for interviews.[80] Unlike NPAs, DPAs require court approval, which is usually granted. Finally, if the government believes a stronger penalty is warranted, it could request that a subsidiary of the company, rather than the parent, enter a guilty plea, which can reduce some of the collateral consequences facing the parent company had it been required to plead guilty.[81] The resolution of the Goldman Sachs FCPA charges, in which the bank's Malaysian's subsidiary pleaded guilty to an FCPA charge, is one example.

10.2.2 Suspension and debarment

One consideration in deciding whether a company will plead guilty or otherwise admit wrongdoing is whether the company also faces collateral consequences from doing so.[82] For instance, companies in the healthcare, defence and construction fields are particularly vulnerable because any admissions of wrongdoing could have the collateral consequence of excluding them from eligibility for the government contracts on which their business heavily relies. Furthermore, any admission of wrongdoing could trigger a host of civil litigation from shareholders or other claimants. Similarly in the Employee Retirement Income Security Act (ERISA) sphere, entities that have registered as a qualified professional asset manager, allowing them to work with pension funds and make investments for ERISA clients, may have their status revoked by the Department of Labor if key individuals or the company has been convicted of a crime. Likewise, for companies regulated by the SEC, enforcement actions can result in suspension, debarment, or both, from the securities markets. Furthermore, even if an issuer is not disqualified altogether, it can lose its well-known seasoned issuer status if it has been found to have violated the securities laws. This can have a significant impact on an issuer's ability to

80 DOJ, 'Manhattan U.S. Attorney Announces Criminal Charges Against Industrial Bank Of Korea For Violations Of The Bank Secrecy Act', press release (20 April 2020), available at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-industrial-bank-korea.

81 See DOJ, Justice Manual §§ 9-28.200, 9-28.1100.

82 See id. § 9-28.1100.

© Law Business Research 2021

quickly file registration statements with the SEC and the issuer's ability to appropriately time the market when offering securities for sale.[83]

See Chapter 26 on fines, disgorgement, etc

In July 2019, the SEC announced that it was changing certain rules related to settlement offers to streamline the process for issuers seeking to settle violations of the securities laws and, concurrently, requesting a waiver from certain collateral consequences of such violations. Jay Clayton, the SEC's chairman at the time, announced:

> *Recognizing that a segregated process for considering contemporaneous settlement offers and waiver requests may not produce the best outcome for investors in all circumstances, I believe it is appropriate to make it clear that a settling entity can request that the [SEC] consider an offer of settlement that simultaneously addresses both the underlying enforcement action and any related collateral disqualifications.*[84]

The simultaneous review of offers of settlement and requests for waivers is a noteworthy development because previously the SEC considered these requests separately, resulting in longer delay and uncertainty for issuers it regulates.[85]

Financial cost 10.2.3

While co-operation between company counsel and the DOJ can save scarce government resources, it often represents a significant cost for the company itself. A company may generally be better placed to run an investigation because conceivably it may know where information is housed and whom to talk to, and can more readily determine the relevant facts and documents at issue. Still, running a high-quality, diligent and thorough internal investigation, despite the relative ease of doing so, is expensive. Document review of company emails, hiring external counsel, travel to and from interviews and preparing presentations to the government, all add up to significant expense. Moreover, if individual employees are implicated in the wrongdoing, they may also choose to hire their own counsel who will also perform an investigation, albeit in a more limited fashion, for which the company may bear financial responsibility. Finally, companies that are found to have committed misconduct may also need to reimburse the victims of their misconduct for certain expenses or pay restitution, which could be considerable and affect other aspects of an investigation

83 Adam Hakki et al., 'SEC Chairman Announces Significant Changes To Commission Procedures For Considering Disqualification Waivers', Shearman & Sterling (7 August 2019), available at https://www.shearman.com/perspectives/2019/08/sec-chairman-announces-significant-changes-to-commission-procedures.

84 Jay Clayton, Chairman, US Securities and Exchange Commission, 'Statement Regarding Offers of Settlement', Public Statement, (3 July 2019), available at https://www.sec.gov/news/public-statement/clayton-statement-regarding-offers-settlement.

85 Adam Hakki et al., 'SEC Chairman Announces Significant Changes To Commission Procedures For Considering Disqualification Waivers', Shearman & Sterling (see supra note 83).

© Law Business Research 2021

or settlement. For example, in 2016, asset management firm Och-Ziff (now named Sculptor Capital Management) agreed to a US$412 million criminal settlement with the DOJ and SEC for violations of the FCPA.[86] In September 2019, however, a federal judge ruled that certain former investors in a Congolese mine should be classified as victims of Och-Ziff's misconduct, raising the question of whether those investors would be entitled to restitution from the firm.[87] While the investors initially claimed that they were entitled to US$1.8 billion,[88] they ultimately entered into a settlement agreement in September 2020 that entitled them to US$136 million in restitution.[89]

In years past, companies attempted to recoup the costs of their own internal investigations of misconduct by seeking restitution under the Mandatory Victims Restitution Act (MVRA), which requires that certain convicted felons 'reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense'.[90] In May 2018, however, the United States Supreme Court held that the MVRA's provision for reimbursement of investigation expenses applied only to government investigations and not to private investigations undertaken by a victim.[91] The Court explained that the MVRA does not 'cover the costs of a private investigation that the victim chooses on its own to conduct, which are not "incurred during" participation in a government's investigation'.[92] Even if 'the victim shared the results of its private investigation with the Government', that does not mean that the private investigation was 'necessary' under the MVRA.[93]

10.2.4 Disruption to business

Any business executive or in-house counsel will know keenly that an investigation, regardless of whether the company chooses to co-operate with government authorities, will result in some amount of disruption to key business

86 Dylan Tokar, 'Restitution Battle Throws Three-Year-Old Och-Ziff Settlement Into Limbo', *Wall St. J.* (7 September 2019), available at https://www.wsj.com/articles/restitution-battle-throws-three-year-old-och-ziff-settlement-into-limbo-11567810832.

87 Id.

88 Id.

89 Dean Seal, 'Och-Ziff Reaches Tentative Deal in $421.8M Restitution Bid', *Law360* (14 July 2020), available at https://www.law360.com/newyork/articles/1291993/och-ziff-reaches-tentative-deal-in-421-8m-restitution-bid; Marisol Grandi, 'Sculptor Capital unit enters settlement agreement over restitution dispute', S&P Global Market Intelligence (24 September 2020), available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/sculptor-capital-unit-enters-settlement-agreement-over-restitution-dispute-60462203.

90 18 U.S.C. § 3663A(b)(4).

91 *Lagos v. United States*, 138 S. Ct. 1684, 1685-86 (2018).

92 Id.

93 Id.

© Law Business Research 2021

activities. While declining to co-operate with an investigation should not in and of itself indicate an organisation's culpability, it could have negative public relations consequences as investors and other third-party stakeholders may view this as indicative of guilt or the potential magnitude of the financial penalty. The Justice Manual does make clear, however, that 'the decision not to co-operate by a corporation . . . is not itself evidence of misconduct at least where the lack of co-operation does not involve criminal misconduct or demonstrate consciousness of guilt'.[94]

Whether or not a company chooses to co-operate with the government in an investigation, any investigation will cause disruption to the company's daily operations, and may even affect share prices. For example, an investigation can take up executives' time and attention; in-house counsel must coordinate extensively with external counsel; any key witnesses have to set aside time to be prepped and interviewed. In addition, financial resources may need to be diverted to help cover the costs of complying with or conducting an internal investigation.

Furthermore, investigations often bring about significant uncertainty for a business, depending on the seriousness and scale of the investigation. Investors may lose confidence in the company's financial prospects, especially because it may be necessary to divulge details related to the investigation to lenders and other third-party finance partners even before the investigation has been concluded (including details that have not been disclosed publicly). In the event that a company is facing the prospect of paying a substantial financial penalty in an investigation, lenders may choose to withdraw funding or revaluate the terms of any outstanding loans, causing the company's share price to drop accordingly.[95]

Exposure to civil litigation 10.2.5

Companies that co-operate with the government are often at risk of follow-on civil litigation based on any admissions or acceptance of lesser charges in connection with an investigation. Many investigations result in companies making certain admissions to the government, which potential plaintiffs can use to base any civil ligation on, either through class or derivative actions. These civil actions can also have significant financial ramifications. For example, civil penalties in the antitrust sphere can result in treble damages.[96] Because of the associated risks of derivative civil actions, companies may ultimately decide that the cost of co-operation is simply too high, and instead decline to co-operate, deny liability and risk defending the company's innocence at trial.

94 DOJ, Justice Manual § 9-28.700.

95 See, e.g., DOJ, Justice Manual § 9-28.700 ('a protracted government investigation . . . could disrupt the corporation's business operations or even depress its stock price').

96 15 U.S.C. § 15(a).

© Law Business Research 2021

A government investigation or admission of guilt may only be the first stage of a company's legal issues. For example, in 2014, following an investigation, the SEC charged Avon Products with having violated the FCPA for failing to put in place comprehensive controls for detecting instances of bribery in China. Avon settled the civil and criminal cases by agreeing to a fine of US$135 million. This resulted in shareholders filing several securities class action lawsuits against the company, claiming that Avon's management failed to put in place adequate controls to prevent FCPA violations, causing the company to lose millions of dollars of shareholder money through the cost of the related investigations and government fines. Ultimately, the case was dismissed because the court declined to find that the FCPA created a private right of action; however, defending the follow-on civil litigation had cost yet more resources and time.[97]

VEON (formerly known as VimpelCom) faced similar ramifications following a government investigation in 2017. VEON's share price dropped after it disclosed that it was under investigation by US and Dutch government authorities for potential FCPA violations and was conducting its own internal investigation. Ultimately, VEON entered into a DPA with the US government and paid roughly US$460 million in penalties. Additionally, the company had spent nearly US$900 million in related investigation and litigation costs. VEON shareholders brought a securities fraud action against the company, claiming that it had failed to disclose that the company's gains were the result of bribes paid to foreign governments in violation of the FCPA. The plaintiffs relied on certain admissions that VEON had made in connection with its DPA, which the court ultimately decided were actionable.[98]

See Chapter 35 on parallel civil litigation

10.2.6 Excessive co-operation between counsel and the government

At what point is co-operation and coordination between the DOJ and company counsel too much? Sometimes a company's internal investigation becomes so entangled with a government investigation and government and company counsel are so coordinated, that it appears as if the government has 'outsourced' its investigatory authority. This can cause problems later down the line. For example, a company's investigation records could become subject to discovery in a criminal case against one of its employees, even if those records would otherwise be considered privileged. Additionally, a court could decide to exclude certain evidence or testimony in the criminal case for running afoul of certain constitutional provisions, even if that testimony was elicited by company counsel and not the government.

97 Benjamin Galdston, 'Shareholder Litigation for Waste of Corporate Assets in Internal FCPA Investigations', *The Review of Securities & Commodities Regulation* (18 April 2018), available at https://s3.amazonaws.com/documents.lexology.com/9877aa80-bdfa-49fb-871b-734a74300baa.pdf.

98 Id.

© Law Business Research 2021

Such complications from perceived 'outsourcing' of criminal investigations to the private sector have resulted in judicial oversight of internal investigations, which would otherwise be rare. In *United States v. Connolly*, for example, Gavin Campbell Black, a former Deutsche Bank trader who was charged with unlawfully manipulating LIBOR interest rates, moved to suppress statements he had made in connection with Deutsche Bank's internal investigation of his trading activity and that of other traders.[99] Black argued that, because the DOJ had effectively 'outsourced' its own investigation function to Deutsche Bank's company counsel, his statements had actually been compelled by the US government in violation of his right against self-incrimination. The underlying investigation – which included interviews with Black and other traders – involved allegations that several banks, including Deutsche Bank, unlawfully manipulated the setting of LIBOR interest rates, and Deutsche Bank eventually entered into a DPA with the DOJ. Because Black's statements were not used at his criminal trial, before the grand jury or during its investigation, Judge McMahon found that Black's right against self-incrimination was not actually violated. She did, however, conclude that Deutsche Bank's company counsel had essentially become an arm of the DOJ, writing that:

> *[R]ather than conduct its own investigation, the Government outsourced the important developmental stage of its investigation to Deutsche Bank – the original target of that investigation . . . Deutsche Bank . . . effectively deposed their employees by company counsel and then turned over the resulting questions and answers to the investigating agencies.*[100]

Judge McMahon's findings underscore the need for the DOJ and company counsel to maintain their independence during an internal investigation, lest the company become a *de facto* part of the prosecution team. Given widespread sensitivity to the issue, it is unlikely that the line between an independent but appropriately coordinated investigation, and an excessively outsourced investigation, will actually be crossed, but defendants may well continue to raise outsourcing arguments when they see an opening to demand additional discovery from the DOJ as well as the company. To steer clear of this risk, company counsel are advised to carefully evaluate (and re-evaluate) their relationship to the government and ensure that they are keenly aware of how their fiduciary duties may differ from and conflict with those of the government.

Other options besides co-operation 10.2.7

Co-operation is not the only option for companies or individuals when facing a government investigation. While companies that co-operate are generally

99 No. 16 Cr. 0370 (CM) (ECF No. 432), 2019 WL 2120523 (S.D.N.Y. 2 May 2019) (Opinion Denying Defendant Gavin Black's Motion for *Kastigar* Relief).

100 Id.

© Law Business Research 2021

guaranteed some degree of leniency, there are situations in which co-operation many not effectively prevent prosecution or reduce a financial penalty, which the Justice Manual guidelines themselves acknowledge: 'The government may charge even the most cooperative corporation . . . if . . . the prosecutor determines that a charge is required in the interests of justice. Put differently, even the most sincere and thorough effort to cooperate cannot necessarily absolve a corporation that has . . . engaged in an egregious, orchestrated, and widespread fraud.'[101] Therefore, there are situations when it is actually pointless to pursue co-operation and other methods must be employed.

First, the company can request a meeting with authorities to explain why the allegations do not amount to an actual violation of law or the particular agency does not have jurisdiction. Second, the defendant could challenge the jurisdiction of the court or regulator's jurisdiction to investigate the matter. Third, companies always have the option to fight the charges on the merits based on insufficiency of evidence in a court of law. This method was employed to dramatic effect by FedEx, when it refused to settle charges that it had conspired to ship illegal prescription drugs to online pharmacies.[102] Just four days into the trial, the DOJ voluntarily dismissed the charges, because it had insufficient evidence to proceed.[103] Meanwhile, United Parcel Service, Google, Walgreens Company and CVS Caremark Corporation had to pay hefty fines after settling with the government.[104]

10.3 Special challenges with multi-agency and cross-border investigations

10.3.1 Multi-agency coordination

Multi-agency coordination is a crucial element of successfully resolving any large, corporate investigation in which multiple US agencies are involved. In 2012, the DOJ issued guidance, which solidified long-standing agency practice, to ensure that 'Department prosecutors and civil attorneys coordinate together and with agency attorneys in a manner that adequately takes into account the government's criminal, civil, regulatory and administrative

101 DOJ, Justice Manual § 9-28.720.

102 Dan Levine, 'US Ends $1.6 billion Criminal Case Against FedEx', Reuters (17 June 2016), available at https://www.reuters.com/article/us-fedex-pharmaceuticals-judgment-idUSKCN0Z32HC.

103 Id.; Dan Levine and David Ingram, 'US Prosecutors Launch Review of Failed FedEx drug case', Reuters (15 July 2016), available at https://www.reuters.com/article/us-fedex-doj-idUSKCN0ZV0GO.

104 Dan Levine & David Ingram, 'US Prosecutors Launch Review of Failed FedEx drug case', Reuters (see supra note 103); Alicia Mundy and Thomas Catan, 'Pain-Pill Probe Targets FedEx, UPS', *Wall St. J.* (15 November 2012), available at https://www.wsj.com/articles/SB10001424127887324595904578121461533102062.

© Law Business Research 2021

remedies'.[105] The policy statement emphasises 'that criminal prosecutors and civil trial counsel should timely communicate, coordinate, and cooperate with one another and agency attorneys to the fullest extent appropriate to the case and permissible by law' by ensuring that 'criminal, civil, and agency attorneys coordinate in a timely fashion, discuss common issues that may impact each matter, and proceed in a manner that allows information to be shared to the fullest extent appropriate to the case and permissible by law'.[106] Furthermore, the Justice Manual has policies obliging departmental attorneys to consider the possibility of any parallel proceeding '[f]rom the moment of case intake' and discuss remedies and communication with other interested investigatory agents and to 'consider investigative strategies that maximize the government's ability to share information among' various agencies.[107] Additionally, the Justice Manual directs prosecutors to assess '[a]t every point between case intake and final resolution . . . the potential impact of [agency] actions on criminal, civil, regulatory, and administrative proceedings'.[108]

In practice, each agency has its own processes and time frames for investigating alleged misconduct and approving settlements. As a result, on occasion, it can be difficult for agencies to effectively communicate and coordinate on a particular investigation such that multi-agency resolutions are reached simultaneously. In this regard, a company that co-operates with all of the relevant government agencies could play a role in encouraging agencies to coordinate by ensuring they are aware of each agency's progress in the investigation and settlement discussions, and encouraging agencies to communicate, when appropriate.

See Chapter 24 on negotiating global settlements

Cross-border coordination 10.3.2

Coordination between international law enforcement agencies has only grown in recent years. In 2018, the DOJ announced that FCPA cases typically involve between four and five different international agencies, particularly because many of the largest DOJ bribery cases target foreign companies in coordination with foreign authorities.[109]

105 US Att'y Gen., 'Memorandum for all United States Attorneys, Director, Federal Bureau of Investigation, All Assistant United States Attorneys, All Litigating Divisions, All Trial Attorneys', DOJ (30 January 2012), available at https://www.justice.gov/jm/organization-and-functions-manual-27-parallel-proceedings.

106 Id.

107 DOJ, Justice Manual § 1-12.000.

108 Id.

109 Evan Norris, 'How Enforcement Authorities Interact', Global Investigations Review (19 August 2019), available at https://globalinvestigationsreview.com/chapter/1196461/how-enforcement-authorities-interact. See also DOJ, 'Airbus Agrees to Pay Over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case', press release (31 January 2020), available at https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case (recognising that the largest global foreign

© Law Business Research 2021

Cross-border investigations may present special challenges and opportunities in comparison to single-jurisdiction investigations. A recent trend apparent in large, corporate investigations is the increased level of coordination and co-operation between various law enforcement agencies. This coordination may come in the form of official, administrative channels such as mutual legal assistance treaties (MLATs), memoranda of understanding, or specific agreements between countries in relation to particular subjects.[110]

The MLAT process has undergone significant reform in recent years, in response to the oft-criticised laborious nature of preparing the requests and having them fulfilled. In December 2017, Jeff Sessions, then US Attorney General, called on the international law enforcement community to 'expedite mutual legal assistance requests', stating: 'If [requests for information are] not properly shared between nations, then, in many cases, justice cannot be done. It is essential that we continue to improve that kind of sharing'.[111] In accordance with this commitment to improve information sharing between the DOJ and other international law enforcement agencies, the DOJ has (1) allocated increased resources to the office responsible for handing MLAT requests and (2) established a cyber unit to process requests for electronic evidence.[112] Aligning with the DOJ's efforts, Congress passed the Anti-Money Laundering Act of 2020 (AML Act),[113] which, among other things, authorises the DOJ and the US Department of the Treasury to obtain foreign bank records during criminal investigations and in civil forfeiture actions.[114] Specifically, under the AML Act, regulators can issue subpoenas to any foreign bank that maintains a correspondent account in the United States to request records maintained abroad.[115] This provides regulators with an alternative to the MLAT process to obtain foreign records, but it remains to be seen how regulators will use this power in practice.

In addition to these formal channels, however, international law enforcement agencies may also informally choose to share investigative strategies,

---

bribery resolution to date was made 'possible thanks to the dedicated efforts of [the DOJ's] foreign partners at the Serious Fraud Office in the United Kingdom and the PNF in France', and noting that 'the department has taken into account these countries' determination of the appropriate resolution into all aspects of the US resolution').

110 Id.

111 Jeff Sessions, Att'y Gen., DOJ, Remarks at the Global Forum on Asset Recovery Hosted by the United States and the United Kingdom' (4 December 2017), available at https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-global-forum-asset-recovery-hosted-united.

112 Id.; Evan Norris, 'How Enforcement Authorities Interact', Global Investigations Review (see supra note 109).

113 31 U.S.C. § 5323.

114 See Andrey Spektor, 'How Anti-Corruption Push Affects US Cos. Operating Abroad' (27 July 2021), available at https://www.law360.com/articles/1406849/how-anti-corruption-push-affects-us-cos-operating-abroad.

115 See 31 U.S.C. § 5318(k)(3)(A)(i).

© Law Business Research 2021

information and access to information and witnesses within their respective jurisdictions. One notable innovation has been the use of text messaging between various prosecutorial agencies to compare evidence and coordinate simultaneous raids.[116] For example, in 2016, Brazilian and French prosecutors used WhatsApp to communicate in advance of the raids at the 2016 Rio Olympic Games.[117] Informal coordination presents obvious upsides to the US government. Instead of relying on slow and burdensome official processes for co-operation, informal co-operation allows US authorities to gain the benefits of shared knowledge in an expedient manner, more akin to the fast-paced nature of the wrongdoer's misconduct in large, complex cross-border investigations.

For companies, this increased co-operation changes the calculus of whether and how to co-operate with authorities, precisely because information that is shared in one jurisdiction may easily and quickly become known in another jurisdiction, potentially with different criteria for liability.

See Chapter 11 on production of information to authorities

DOJ's policy against 'piling on' 10.3.3

Piling on can negatively affect the morale of companies, investors and customers and can often mean that companies seldom have a sense of finality when it comes to investigations brought by an alphabet soup of different law enforcement agencies or regulatory agencies.

Given the number of different government agencies, both foreign and domestic, that could have an interest in any given investigation, in May 2018, Deputy Attorney General Rod Rosenstein announced the DOJ's new policy against 'piling on', which favours a less aggressive approach to cumulative prosecution. In describing this new policy, Rosenstein stated that the DOJ should 'discourage disproportionate enforcement of laws by multiple authorities', likening it to the football practice of multiple players 'piling on' after a player has already been tackled.[118] He added: 'Our new policy discourages "piling on" by instructing Department [of Justice] components to appropriately coordinate with one another and with other enforcement agencies in imposing multiple penalties on a company in relation to investigations of the same misconduct', noting that often large, regulated companies are accountable to 'multiple regulatory bodies', which creates the risk of duplicative and onerous punishments beyond 'what is necessary to rectify the harm and deter future violations'.[119]

116 Evan Norris, 'How Enforcement Authorities Interact', Global Investigations Review (see supra note 109).

117 See Clara Hudson, 'GIR Live: Brazilian Prosecutor Says WhatsApp Chat Group Drove Investigation Forward', Global Investigations Review (27 October 2017), available at https://globalinvestigationsreview.com/article/1149463/gir-live-brazilian-prosecutor-says-whatsapp-chat-group-drove-investigation-forward.

118 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

119 Id.

© Law Business Research 2021

Under this new policy, the DOJ now considers 'the totality of fines, penalties, and/or forfeiture imposed by' all enforcement agencies to avoid excessive punishment.[120] Moreover, Rosenstein emphasised that the new policy reinforces the following core policies: ensuring that the federal government (1) does not use its enforcement power for impermissible purposes (i.e., leveraging the threat of criminal prosecution to induce a company to settle a civil case), (2) encourages intra-governmental coordination to ensure an 'overall equitable result', (3) encourages DOJ officials to coordinate with other DOJ officials, and (4) specifies concrete factors that the DOJ will evaluate in the event that a case does warrant multiple penalties.[121]

In the enforcement of the FCPA, in particular, it has been long-standing practice for the DOJ and SEC to coordinate their investigations and ensuing resolutions; however, the formalisation of the anti-piling-on policy indicates that this practice will become more commonplace in other legal arenas.

Indeed, since former Deputy Attorney General Rod Rosenstein's announcement of the anti-piling on policy in May 2018, there have been several corporate settlements involving federal and state prosecutors and regulators that reflect this policy. For example, in April 2019, Standard Chartered Bank reached a settlement with the DOJ, the Department of the Treasury's Office of Foreign Assets Control (OFAC), the Federal Reserve Board of Governors, New York State prosecutors and regulators and the UK's Financial Conduct Authority, regarding sanctions violations.[122] Standard Chartered agreed to pay more than US$1 billion in penalties, fines and forfeiture to these different authorities.[123] The DOJ agreed to 'credit a portion' of the related payments to other authorities, and after crediting received US$52 million in fines and US$240 million in forfeiture. OFAC assessed a separate civil penalty of US$639 million, which was deemed satisfied by the payments to the DOJ and the Federal Reserve Board of Governors.[124] In another example, in August 2020, the DOJ declined to prosecute consumer loan company World Acceptance Corporation for

120 Memorandum from Rod J Rosenstein, Deputy Att'y Gen., DOJ, to Heads of Department Components and United States Attorneys (9 May 2018), available at https://www.justice.gov/opa/speech/file/1061186/download#:~:text=In%20reaching%20corporate%20resolutions%2C%20the,to%20achieve%20an%20equitable%20result.

121 Rod J Rosenstein, Deputy Att'y Gen., DOJ, Remarks to the New York City Bar White Collar Crime Institute (see supra note 118).

122 DOJ, 'Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion', press release (9 April 2019), available at https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions#:~:text=Standard%20Chartered%20Bank%20(SCB)%2C,two%20years%20for%20conspiring%20to.

123 Id.

124 OFAC, press release, 'U.S. Treasury Department Announces Settlement with Standard Chartered Bank' (9 April 2019) available at https://home.treasury.gov/news/press-releases/sm647#:~:text=WASHINGTON%20%E2%80%93%20As%20part%20of%20a,settle%20its%20potential%20civil%20liability.

© Law Business Research 2021

violations of the FCPA, in part because the corporation had agreed to disgorge to the SEC the full amount of its ill-gotten gains.[125] World Acceptance agreed to pay US$21.7 million in disgorgement, penalties and prejudgment interest to the SEC to settle the same FCPA violations.[126]

The DOJ's anti-piling-on policy can also be used as a defence by corporations against perceived duplicative charges by various government agencies. Volkswagen AG, the car manufacturer facing charges by the SEC for failing to disclose its clean diesel emission cheating scheme in a bond offering, successfully narrowed the scope of the SEC's civil suit by arguing that the SEC cannot 'pile on' more charges after the company had already pleaded guilty to three felonies and paid US$25 billion in fines, penalties and settlements to US and state authorities, as well as car owners and dealers, in connection to the alleged misconduct.[127] Indeed, the judge presiding over the case dismissed several claims against Volkswagen, finding that its settlement with the DOJ had already released Volkswagen from any government-filed civil claims arising out of the same underlying fraud.[128] In addition, the judge had questioned why the SEC brought its case against Volkswagen two years after the company resolved the matter with the DOJ.[129]

125 Letter agreement between DOJ and World Acceptance Corp. (5 August 2020), available at https://www.justice.gov/criminal-fraud/file/1301826/download.

126 US Securities and Exchange Commission, press release, 'SEC Charges Consumer Loan Company With FCPA Violations' (6 August 2020), available at https://www.sec.gov/news/press-release/2020-177.

127 Dean Seal, 'VW, But Not Ex-CEO, Dodges SEC's Emissions Fraud Claims', *Law360* (20 August 2020), available at https://www.law360.com/articles/1303103/vw-but-not-ex-ceo-dodges-sec-s-emissions-fraud-claims.

128 Id.

129 David Shepardson, 'US Judge Urges VW, SEC to Resolve Civil Dieselgate Suit', Reuters (16 August 2019), available at https://www.reuters.com/article/us-volkswagen-emissions/u-s-judge-urges-vw-sec-to-resolve-civil-dieselgate-suit-idUSKCN1V61SN.

© Law Business Research 2021

11

Production of Information to the Authorities

Pamela Reddy, Kevin Harnisch, Katie Stephen, Andrew Reeves and Ilana Sinkin[1]

11.1 Introduction

The production of information to authorities is often rife with legal and practical issues that need to be tackled carefully but quickly. Taking control of the process and engaging with regulators early on can focus the information request and help to establish a positive and more productive relationship. In many cases, a regulator will welcome the assistance of the company and its advisers in scoping and prioritising the regulator's receipt of data (and this may result in significant cost savings for the company).

It is important to engage with the regulator as soon as possible and to establish its internal drivers and deadlines, as well as any immediate priorities within the data it has sought. Prioritising may provide more time to work on the broader production (while giving authorities what they need to progress their investigation and satisfy their stakeholders). Engaging with authorities early may also allow the company to find out more about the underlying investigation.

Approaching information requests methodically helps to ensure that all key issues are worked through. Immediate issues to consider include:

- whether the company is the subject of the investigation and any immediate consequences in terms of required notifications and internal communications;
- the powers under which the request is made (and whether what has been requested falls within those powers, including in terms of where it is located);

1 Pamela Reddy, Kevin Harnisch, Katie Stephen and Andrew Reeves are partners, and Ilana Sinkin is a senior associate, at Norton Rose Fulbright LLP.

© Law Business Research 2021

- whether the information is required or merely requested (and whether the company wants to seek a compelled request to help deal with any potential issues arising from voluntary disclosure such as data privacy or confidentiality concerns);
- timing (focusing on what can be done within the requested time frame, however tight, tends to lead to a better outcome in terms of obtaining extensions);
- the precise scope of the request (and considering whether clarification or narrowing is required);
- what sources of data may need to be explored (including electronic devices in employees' possession) and the extent to which assistance from custodians may be required;
- the proposed approach to protecting privilege;
- any additional requirements triggered by the data request, such as in relation to data preservation or other reporting;
- to what extent the company plans to review all material before it is provided to the regulator or subsequently;
- where multiple regulators are involved, coordination and ensuring a consistent response and minimising duplication of effort; and
- the impact of local laws on the collection, review and production of data (including whether the process of responding will involve any issues arising from cross-border transmission of data).

Cost and proportionality are key issues in data productions. While most companies will want to be co-operative, it is also important that data is not needlessly collected, hosted, reviewed and produced. Data sources and volumes are ever increasing and seemingly small decisions (e.g., as to the number of custodians, date ranges or precise search terms) can have a significant impact on the overall cost of the production and ongoing hosting (as well as the usefulness of the data for the regulator). Where broad search terms are required or applied in the first instance, review of a sample of the results or a technology-assisted review might enable narrowing of the searches. Equally, the approach to privilege reviews can have a big impact on cost. In some circumstances, a non-exhaustive technology-driven process may be appropriate combined (in some jurisdictions) with putting in place a clawback agreement with the regulators.

The technical details are important when it comes to data collection. Time spent working through IT infrastructure, device history, the status of former employees' data, and so on, optimises collection and can help to reduce costs in the long term. It is also crucial that collection and production IT requirements are fully understood and that any uncertainties are flushed out to avoid document productions needing to be rerun later down the line.

Increasingly document and information requests cover not only documents and emails, but also other electronic records such as SMS, WhatsApp and similar messages and voice notes (which may be less easily searchable).

© Law Business Research 2021

The move to increased remote working accelerated by the covid-19 pandemic has generated a greater volume and variety of potentially responsive electronic communications while also hindering the process of responding to information requests. Great care needs to be taken to ensure that all relevant data is preserved, including data and devices held off-site.

In this chapter we set out key considerations when responding to document requests from UK and US regulators and important issues to be considered when conducting reviews and making productions.

11.2 UK regulators

11.2.1 Powers of the Serious Fraud Office

The key power available to the Serious Fraud Office (SFO) is to require documents or information under a notice pursuant to section 2 of the Criminal Justice Act 1987 (CJA) (a section 2 notice).

The SFO can compel a person (individual or corporate) it has begun investigating[2] and any other person whom it believes may have information which is relevant to that investigation, to produce documents or information recorded in any form with respect to 'any matter relevant to the investigation'.[3] There is no 'right to silence' (although where an individual provides information during a compelled interview, that information cannot, except in very limited circumstances, later be used against that individual during a prosecution).

Failure to comply with a section 2 notice is a criminal offence that can result in imprisonment for a term of up to six months or a fine, or both.[4] The only defence is where there is a 'reasonable excuse' for the non-compliance but this is likely to be very narrowly construed. The key exception to the provision of documents is where documents are protected by legal professional privilege. The SFO has stated in its Corporate Co-operation Guidance[5] that it expects companies producing documents to obtain independent certification that withheld material is privileged, and it has indicated on various occasions that it views waiver of privilege as an indicator of co-operation (although it has stressed that it does not require waiver).

In February 2021, the UK Supreme Court ruled that section 2(3) of the CJA does not have extraterritorial effect.[6] This means that a section 2 notice cannot be used to compel a foreign company that does not carry on business in the United Kingdom to produce documents held outside the country. The SFO will have to obtain any such documents via mutual legal assistance (MLA).

---

2 The powers can also be used before the SFO has opened an investigation where it appears to the Director of the SFO that conduct that may constitute an offence under the UK Bribery Act 2010, ss.1, 2 or 6 may have taken place (CJA, s.2A).

3 CJA, s.2(2).

4 ibid., s.2(13).

5 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/corporate-co-operation-guidance/.

6 *R (KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2.

© Law Business Research 2021

Although the section 2 powers are broad, the scope and timing of the response to section 2 notices is nearly always a matter of negotiation.

Powers of other authorities 11.2.2

Various other authorities may require documents to be produced. The powers of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) are dealt with in more detail below. The National Crime Agency (NCA) and Her Majesty's Revenue and Customs (HMRC) can require an individual to provide information, documents or communications in their possession pursuant to a disclosure notice issued under section 62 of the Serious Organised Crime and Police Act 2005 (SOCPA). A disclosure notice can be issued if it appears that there are reasonable grounds for suspecting that a relevant offence (such as failure to prevent facilitation of tax evasion or money laundering) has been committed and that any person has information relating to a matter relevant to the investigation of that offence that is likely to be of substantial value to that investigation. A person who fails to comply commits an offence under section 67(1) SOCPA and a conviction can result in fines or imprisonment of up to two years.

There are exceptions to the provision of documents for legally privileged documents and confidential banking information. Certain categories of material that a person cannot be required to provide are set out in the Police and Criminal Evidence Act 1984 (PACE).[7] There is also no right to silence in an interview compelled under section 62 SOCPA.

Where there has been failure to comply with a request under section 62 SOCPA, or where giving a notice under section 62 may be prejudicial to the investigation, under section 66 SOCPA, both HMRC and the NCA can apply before a magistrate for a search warrant.

The Proceeds of Crime Act 2002 also provides mechanisms, such as production orders, for obtaining documents.[8] In addition, there are various powers within PACE that allow authorities to search the premises for documents.

FCA and PRA 11.2.3

Compulsory requests 11.2.3.1

In its Enforcement Guide, the FCA states that its standard practice is to use statutory powers to require the production of information or documents.[9] The FCA and PRA both have a general power in support of their supervisory and enforcement functions[10] to compel the production of information and documents.[11] This allows the regulators to request in writing that 'author-

7 Police and Criminal Evidence Act 1984, s.11.

8 Proceeds of Crime Act 2002, s.345.

9 FCA Enforcement Guide [EG], EG 4.7.1.

10 EG 3.2.1.

11 Financial Services and Markets Act 2000 (FSMA), s.165.

© Law Business Research 2021

ised persons'[12] or persons connected with authorised persons provide specified information or documents that are 'reasonably required' in connection with the regulator's statutory powers.[13] The definition of 'connected with' is broad and includes group members, parent undertakings and employees of authorised persons. The FCA and PRA can stipulate (1) the form in which the information is provided[14] and (2) that the information or document is verified or produced to be authenticated.[15]

The regulators also have separate powers for the production of information and documents in connection with investigations.[16] Depending on the matters being investigated, in addition to being able to require the production of relevant information and documents by the person under investigation or any connected person, the FCA and PRA may require another person to produce information or documents in specified circumstances. The FCA or PRA can also use its powers to assist an overseas regulator.[17]

A company may resist disclosure requested by the FCA or PRA using its compulsory powers, where (1) the relevant material is a 'protected item' (under the statutory definition within the Financial Services and Markets Act 2000 (FSMA))[18] or (2) the information or document is not within the scope of the request.

Failure to comply with the request may be treated as a 'serious form of non-cooperation' and as contempt of court and may give rise to a Principle or Conduct Rule breach.[19]

11.2.3.2 Voluntary production

The FCA Enforcement Guide explains that it will sometimes be appropriate to depart from the FCA's standard practice of using its statutory powers to obtain information and documents such as for suspects in criminal or market

12 Firms authorised by the FCA to provide regulated financial services as defined in FSMA, s.31.

13 See also FSMA, s.175.

14 ibid., s.165(5).

15 ibid., s.165(6).

16 ibid., s.167 (general investigations), s.168 (specific investigations), ss.171 to 173.

17 ibid., s.169; EG 3.7.

18 s.413 – '(2) "Protected items" means – (a) communications between a professional legal adviser and his client or any person representing his client which fall within subsection (3); (b) communications between a professional legal adviser, his client or any person representing his client and any other person which fall within subsection (3) (as a result of paragraph (b) of that subsection); (c) items which – (i) are enclosed with, or referred to in, such communications; (ii) fall within subsection (3); and (iii) are in the possession of a person entitled to possession of them. (3) A communication or item falls within this subsection if it is made – (a) in connection with the giving of legal advice to the client; or (b) in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings.'

19 EG 4.7.4 – the FCA may bring proceedings for breach of Principle 11, Statement of Principle 4 or FCA Code of Conduct Handbook (COCON) 2.1.3R.

© Law Business Research 2021

abuse investigations.[20] In connection with the use of statutory powers to require the production of documents, the provision of information and the answering of questions regulated firms and certain individuals must be open and co-operative with the FCA and PRA when responding.[21] Regulated firms and approved persons such as senior managers are also expected to proactively disclose to the FCA or PRA anything of which the regulator would reasonably expect notice.[22] The FCA also encourages voluntary production of information such as reports from internal investigations.[23]

The level of co-operation is taken into account by the FCA and PRA when deciding whether to bring enforcement action and when determining any penalty. However, prior to making voluntary disclosure, firms should consider any other relevant obligations such as duties of confidentiality and data protection requirements.

FCA and PRA obligations 11.2.3.3

FSMA restricts the disclosure by the FCA or PRA of information relating to a firm's business where such information is confidential and has been received for the purposes of the authority's functions.[24] It is a criminal offence to make an unauthorised disclosure, but there are a number of exceptions, including where prescribed 'gateways' apply such as disclosure to overseas regulators.

Information Commissioner's Office 11.2.4

As data breaches become more prevalent and companies recognise the extent of potential liability following high-profile cases in 2020 involving British Airways and Marriott, considerations regarding the provision of information to regulators, enforcement agencies and other third parties are becoming increasingly important.

Following the submission of a personal data breach form, there are typically numerous rounds of questions from the Information Commissioner's Office (ICO) should it decide to investigate. The purpose of these questions

20 EG 4.7.1: 'In such a case, the interviewee does not have to answer but if they do, those answers may be used against them in subsequent proceedings, including criminal or market abuse proceedings.'

21 See the FCA's reminder in its Enforcement Guide at EG 4.7.2.

22 Principle 11 of the FCA's Principles for Businesses, Fundamental Rule 7 of the Prudential Regulation Authority's Fundamental Rules. There are a number of enforcement outcomes relating to breaches of these provisions; e.g., *The Bank of Tokyo Mitsubishi UFJ Limited and MUFG Securities EMEA plc*, February 2017, available at https://www.bankofengland.co.uk/news/2017/february/pra-imposes-fine-on-the-bank-of-tokyo-mitsubishi-ufj-limited-and-fine-on-mufg-securities-emea-plc, and Bank of Scotland plc, June 2019, available at https://www.fca.org.uk/publication/final-notices/bank-of-scotland-2019.pdf. In relation to senior managers see Senior Manager Conduct Rule SC4 in COCON 2.2.4R.

23 EG 3.1.2, EG 3.11.

24 FSMA, s.348.

© Law Business Research 2021

is not only to understand more about the breach and establish whether the rights of data subjects have been adequately protected, but also to understand more about the company's technical and organisational measures at the time of the breach to assess whether the EU General Data Protection Regulation has been infringed. These requests for information are typically made on an informal basis. However, the ICO may compel the production of information via an information notice under section 142(1) of the Data Protection Act 2018 (DPA). Failure to comply can result in the issuance of a penalty notice under section 155(1)(b) DPA.

Companies should, however, be alive to the potential ramifications of disclosing certain information should subsequent litigation commence, for example in the form of third-party security provider disputes or class actions brought on behalf of data subjects. Companies at the outset of a data breach investigation should consider whether any documents produced could be protected by legal professional privilege (under section 143(4) DPA or common law) and to what extent companies can and should exercise that right. Carefully considering the privilege position is even more important in light of recent draft statutory guidance published by the ICO on 1 October 2020, which provides that the ICO may obtain privileged communications unrelated to data protection legislation in certain circumstances. Until this guidance has been approved by Parliament and put in practice, it remains to be seen whether there will be a significant departure from the ICO's current approach to privileged communications as set out in its Regulatory Action Policy.

Production of documents to other authorities, for example the NCA and FCA, also needs to be considered when investigating and managing large data breaches. The NCA's approach to companies that have suffered a cyberattack differs to its approach when investigating a company of wrongdoing where it seeks to bring a prosecution against the perpetrator. The NCA does not typically have the power to compel a company to co-operate with its investigation by producing documents or answering questions in this context, so it is the company's decision whether to engage with the NCA. In general, the NCA does not voluntarily provide information on a data-breach investigation to the ICO, and it is not a public authority for the purposes of the Freedom of Information Act 2000. However, companies should bear in mind that the ICO does have powers under Part 6 of the DPA to oblige third parties to respond, and material provided to the NCA could be made public in the event of a prosecution.

See Chapters 40 on data protection and 41 on cybersecurity

11.2.5 The Pensions Regulator

The Pension Schemes Act 2021 has introduced new information-gathering powers. It enables the Pensions Regulator to require by notice in writing a person likely to hold information relevant to the exercise of the regulator's

© Law Business Research 2021

powers to attend an interview before the regulator.[25] Failure to attend the interview or to answer questions, without a reasonable excuse, is a criminal offence.[26] This new power is enforceable by a series of escalating fines of up to £10,000 a day.[27]

US regulators 11.3

In the United States, most federal agencies have statutory authorisation to issue administrative subpoenas to compel individuals and entities to produce documents and testimony without prior approval from a court or grand jury.[28]

The US Supreme Court has broadly upheld the use of administrative subpoenas (subpoenas issued by a federal agency without judicial oversight), holding that the government need only show that the administrative subpoena was issued in good faith.[29] In *United States v. Powell*, the Supreme Court articulated a four-factor test to evaluate whether a subpoena was issued in good faith: (1) the investigation is conducted pursuant to a legitimate purpose; (2) the information requested under the subpoena is relevant to that purpose; (3) the agency does not already have the information that it is seeking with the subpoena; and (4) the agency has followed the necessary administrative steps in issuing the subpoena.[30]

In general, federal courts may enforce administrative subpoenas, and refusal to obey a federal court order to comply with an administrative subpoena can result in a federal district court imposing contempt sanctions for non-compliance. In addition, some statutes authorise the court to assess civil penalties for non-compliance with a subpoena.[31]

While each federal agency has its own unique and statutory regulatory schemes for issuing administrative subpoenas, the US Department of Justice

25 Pensions Act 2004, s.72A(1) .

26 ibid., s.77(1A).

27 ibid., s.77A.

28 See, e.g., 15 U.S.C. § 78dd2(d)(2) (The US Department of Justice (DOJ) is granted statutory authority under the US Foreign Corrupt Practices Act 'to subpoena witnesses, take evidence and require the production of any books, papers, or other document'); 7 U.S.C. § 15 (The US Commodity Futures Trading Commission may 'subpoena witnesses, compel their attendance . . . and require the production of any books, papers, correspondence, memoranda, or other records that the Commission deems relevant or material to the inquiry'); Securities Act of 1933, Pub. L. No.73-22 (as amended), Sec. 19(b) (The US Securities and Exchange Commission may subpoena witnesses, take evidence and require the production of documentary evidence deemed relevant or material to an investigation under the Securities Act. The attendance of witnesses and production of documents may be required from anywhere in the United States or any territory at any designated place of hearing).

29 *United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 313 (1978).

30 379 U.S. 48 (1964).

31 See 42 U.S.C. § 9604(e) (authorising the court to assess civil penalties of up to US$25,000 for each day of continued non-compliance with subpoena issued under Comprehensive Environmental Response, Compensation, and Liability Act authority).

© Law Business Research 2021

(DOJ) is the primary federal agency authorised to enforce federal law and defend the interests of the United States. The DOJ has oversight of several federal law enforcement agencies, including the Federal Bureau of Investigation, and is responsible for investigating instances of fraud and corruption. Section 248 of the Health Insurance Portability and Accountability Act 1996 for example, authorises the Attorney General – the chief lawyer of the US federal government and the leader of the DOJ– to issue subpoenas requesting 'production of certain documents and testimony in investigations related to 'any act or activity involving a federal health care offense'.[32]

In addition, the Inspector General Act 1978 created an Office of Inspector General (OIG) within several federal agencies. These OIGs also conduct investigations and may require, by subpoena, the production of documents and testimony to investigate potential fraud involving recipients of federal funding within their respective agencies. Inspectors General are intended to function independently of the agency head.

When producing documents or testimony to a federal agency the information must be accurate. In the United States, it is a criminal offence, punishable by imprisonment and a fine, to knowingly and wilfully make any materially false statement or document to a federal agency.[33] In addition, a person can be criminally prosecuted for perjury if he or she wilfully provides false testimony under oath to a US regulator.[34] Under the Fifth Amendment to the US Constitution, a natural person (not an entity) may refuse to provide information in response to a subpoena if that information may be self-incriminating.

The Freedom of Information Act (FOIA) generally requires government agencies to disclose information, including documents obtained from third parties, upon request. FOIA, however, contains a number of exceptions, allowing government entities to withhold information obtained in response to an administrative subpoena in certain circumstances. When providing information in response to government requests, the producing party should properly claim the appropriate exemptions from disclosure under FOIA.

11.3.1 Voluntary productions

Despite statutory authority to compel production, there are various reasons why federal agencies will seek voluntary productions from an individual or entity. For example, while the DOJ may issue a grand jury subpoena to 'a subject or a target of the investigation', DOJ attorneys are urged to secure information from

32 See 18 U.S.C.§3486(a)(1)(A)(i)(I).

33 18 U.S.C. § 1001 (Whoever knowingly and wilfully makes any materially false statement or writing or document in connection with any matter before the US government may be imprisoned and fined).

34 18 U.S.C. § 1621 (In certain cases, if any person wilfully provides information as true which he does not believe to be true is guilty of perjury).

© Law Business Research 2021

a target of an investigation through voluntary means prior to obtaining a grand jury subpoena because a subpoena 'may carry the appearance of unfairness'.[35]

In addition, the DOJ has issued various policies providing incentives for companies and individuals to voluntarily disclose information. For example, the DOJ Criminal Division's Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy provides that the DOJ may decline to prosecute a company that (1) voluntarily self-discloses misconduct in an FCPA matter, (2) fully co-operates with the DOJ's investigation, and (3) remediates the misconduct in an appropriate and timely manner.[36] The DOJ's Criminal Division has expanded this policy beyond FCPA matters, including in cases involving healthcare and financial fraud.[37] Other agencies provide similar incentives for voluntary co-operation.

If a company is producing documents voluntarily, the company should pay considerable attention to potential disclosure of privileged information. Courts have held that the voluntary submission of privileged materials waives privilege in the United States, whereas a submission made under compulsion does not.[38] In assessing whether the disclosure of privileged documents to regulators was involuntary, courts consider a number of factors, including whether (1) the disclosure was made in response to a court order or subpoena or demand of a government authority, (2) the disclosing party would be subject to penalties if it failed to produce the documents, and (3) the disclosing party objected to the disclosure and asserted any available privilege protections over the documents.[39]

Privilege 11.4

Under English law, communications subject to legal professional privilege are protected. Subject to very narrow exceptions, third parties, including authorities, cannot compel disclosure of privileged information or documents. This common law protection is also broadly reflected in certain statutory provisions (such as section 413 FSMA), but these are not entirely consistent.

See Chapters 36 and 37 on privilege

35 US DOJ, Justice Manual § 9-11.150 (Justice Manual) ('before a known 'target' is subpoenaed to testify before the grand jury about his or her involvement in the crime under investigation, an effort should be made to secure the target's voluntary appearance').

36 Justice Manual § 9-47.120.

37 See, e.g., Deputy Assistant Att'y Gen. Matthew S Miner, U.S. Dep't of Justice Criminal Div., Remarks at the 5th Annual Global Investigations Review New York Live Event (27 September 2018), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division.

38 See *In re Vitamin Antitrust Litig.*, 2002 WL 35021999, at *28 (D.D.C. 23 January, 2002).

39 Id.

© Law Business Research 2021

Under common law there are two types of legal professional privilege:

- Legal advice privilege protects confidential communications between a lawyer[40] and a client for the dominant purpose of giving or receiving legal advice. 'Client' is construed very narrowly: it includes only those individuals within the organisation who are authorised to give instructions and receive advice on the particular matter. The fact that an employee may be authorised to communicate with the lawyers does not make them the client for privilege purposes.
- Litigation privilege protects confidential communications between the client or lawyer (on the one hand) and third parties (on the other), or documents created by or on behalf of the client or lawyer, which come into existence once litigation is in contemplation or has commenced and which are for the dominant purpose of use in the litigation. Litigation can include other adversarial proceedings, but may not be triggered by a regulatory investigation.

Applying the relevant principles in practice and determining the scope of information that may be withheld from the authorities is often complex and contentious (for example in relation to emails with multiple addresses and regarding attachments). In addition, there are circumstances in which regulators may seek to challenge decisions on privilege or request disclosure of privileged material, such as where internal investigations have been conducted by corporates in relation to potential regulatory problems (to the extent privilege is claimed over documents created during the internal investigation or that set out its findings).

In some circumstances the company may wish to provide privileged material on the basis of a limited waiver (with the right to assert privilege against third parties such as civil litigants), but this must be done carefully and with the benefit of legal advice to avoid inadvertently losing privilege.

In the United States, the attorney–client privilege and work-product doctrine can act as powerful shields in protecting documents from disclosure to US regulators. Generally, the attorney–client privilege protects confidential communications between an individual and his or her attorney that are made for the purpose of obtaining or providing legal advice or assistance. The attorney work-product doctrine applies to documents and information that have been prepared in reasonable anticipation of future litigation, or potentially an enforcement action, as contrasted with documents that are prepared for ordinary business purposes.

After receiving a document request from a regulator, careful consideration should be given to potential privilege issues. Particular care needs to be taken with respect to privilege issues when an internal investigation is concurrent with

40 'Lawyer' includes English solicitors, barristers and foreign lawyers qualified to practise in their own jurisdictions (and their staff acting under their direction). It does not include non-legal professionals giving legal advice but does include in-house lawyers.

© Law Business Research 2021

the document production. This is because during an investigation, documents will usually be created pertaining to all aspects of the investigation, including reports on strategy, notes from employee interviews, forensic accounting reports of the company's books and records, and reports on the ultimate investigation findings. The recipient of the document request and the lawyers involved should act with the utmost caution to best maintain privilege over the investigation documents, but they should also ensure that all non-privileged investigation documents responsive to the document request are provided.

Cross-border investigations and considerations 11.5

Introduction 11.5.1

The United Kingdom and the United States both have comprehensive systems concerning the production of documents through the use of mutual legal assistance treaties (MLATs) and other international agreements, such as extradition agreements. MLATs enable a prosecutor in one country to request a prosecutor from another to gather and provide information; this assistance can include testimony, transferring persons in custody, assisting in proceedings related to asset forfeiture, and any other form of assistance permitted under the laws of the two countries.

In the United Kingdom, co-operation with foreign regulators may (and often does) occur at the prosecutorial level, and the SFO in particular has well-established relationships with the DOJ, the Australian Federal Police, and its European counterparts. All MLAT requests for legal assistance from the United States are sent to a specialist office within the central authority.

The FCA and PRA also have memoranda of understanding (MOUs) with other national and international authorities. In addition, certain US federal agencies have MOUs or exchange letters with their foreign counterparts. For example, the US Treasury's Financial Crimes Enforcement Network has MOUs with financial intelligence agencies in many countries, including the United Kingdom. The US Securities and Exchange Commission (SEC) also has co-operative arrangements with non-US regulators to facilitate co-operation with its counterparts in other countries.[41]

Recent years have witnessed a number of large cross-border investigations; for example, the recent cross-border joint investigation into Airbus resulted in co-ordinated settlements with UK, US and French authorities. A US federal appellate court held in *United States v. Allen*, that evidence derived from compelled testimony in the United Kingdom could not be used in a criminal case in the United States, even if that testimony was lawfully obtained in the United Kingdom.[42] In that decision, the FCA and the DOJ were jointly investigating alleged manipulation of the LIBOR inter-bank lending rate by two former traders. The FCA interviewed two traders and provided their testimony

41 https://www.sec.gov/about/offices/oia/oia_coopfactsheet.htm.

42 *United States v. Allen et al.*, No. 16-898 (2nd Cir. 19 July 2017).

© Law Business Research 2021

to a former banker who co-operated in the DOJ's case against the two traders in the United States. The Second Circuit held that the DOJ had failed to demonstrate that the compelled testimony from the two traders did not taint the banker's testimony against the traders in the grand jury proceeding and the trial, and overturned the convictions. The Second Circuit held that incriminating statements to non-US officials may only be used as evidence in criminal cases in the United States if made voluntarily and the use of the compelled testimony to the FCA as evidence in a US criminal trial would violate the defendants' Fifth Amendment right against self-incrimination.

Notwithstanding that the *Allen* case could raise an impediment to collaboration between US and UK authorities, one can expect co-operation and co-ordination to increase: regulators are increasingly working together to investigate and resolve issues; the ambit of extraterritorial jurisdiction is being continually expanded; and common global standards for effective compliance programmes (whose existence may be a legal or *de facto* defence)[43] are emerging. Practical points for a client facing a multi-jurisdictional or multi-regulator investigation include the need for:

- early consideration of which jurisdictions or authorities may be engaged (various factors such as money laundering legislation and international funds flow may make this number greater than it first appears);
- early and co-ordinated engagement with each authority;
- maintaining clear and comprehensive records relating to production; and
- getting legal advice in each jurisdiction, for example in relation to privilege and data protection.

11.5.2 Information outside the United Kingdom

The UK authorities (including the SFO and FCA or PRA) may seek international assistance from overseas authorities in connection with the exercise of a wide number of investigatory powers, including the production of data from sources and persons outside the United Kingdom. Their powers are contained in the Crime (International Co-operation) Act 2003 (CICA).

Under CICA, an MLA request can only be made if it appears to the investigating authority that there are reasonable grounds for suspecting that an offence has been committed. The request must relate to the obtaining of evidence 'for use in the proceedings or investigation'.[44]

Moreover, the SFO and FCA or PRA can make direct approaches to the relevant authorities in other jurisdictions to obtain evidence directly.

Following a recent UK Supreme Court decision, it is now established that, in addition to MLA, the SFO may also use its coercive powers[45] to compel a UK company to produce documents held outside the jurisdiction and also

43 For example, UK Bribery Act, s.7 provides for the defence of 'adequate procedures'.

44 Crime (International Co-operation) Act 2003, s.7(2).

45 Under CJA 1987, s.2.

© Law Business Research 2021

compel a foreign company that carries on a business in the United Kingdom to produce documents held outside the jurisdiction.[46]

Under the Crime (Overseas Production Orders) Act 2019 certain UK authorities (including the SFO and FCA or PRA) are able to seek a court order (an overseas production order) to compel a person outside the United Kingdom to provide electronic data stored abroad where a designated international co-operation arrangement between the United Kingdom and a foreign state exists. The only such agreement currently in existence is between the United Kingdom and the United States.[47]

Brexit 11.5.3

Following the end of the transition period on 31 December 2020, the United Kingdom is no longer party to the reciprocal and mutual legal assistance provisions contained in EU law.

Requests for MLA between the Member States of the European Union and the United Kingdom are now based on cooperation through the Council of Europe 1959 Convention on Mutual Assistance in Criminal Matters and its two additional protocols, as supplemented by provisions agreed in Title VIII of the EU–UK Trade and Cooperation Agreement.

It seems likely that co-operation between the United Kingdom and the European Union will continue even though the transition period has now ended; although in the absence of new legal provisions, there may well be increased delays in effecting co-operation.

Requests into the United Kingdom 11.5.4

Under CICA, UK authorities may assist overseas authorities via formal MLA requests (including European investigation orders (EIOs)) or through direct information sharing. The UK Central Authority, which forms part of the

46 *R (on the application of KBR, Inc.) v The Director of the Serious Fraud Office* [2021] UKSC 2. At first instance the Administrative Court had held that any foreign company (whether or not it carried on business in the United Kingdom) could be compelled to produce documents where there was a 'sufficient connection between the company and the jurisdiction'. This was overturned by the UK Supreme Court. *In R (on the application of Tony Michael Jimenez) v. (1) First Tier Tax Tribunal and (2) Her Majesty's Commissioners for Revenue and Customs* [2019] Civ 51, the Court of Appeal applied the 'sufficient connection' test set out in the first instance decision in *KBR* in ruling that HMRC was authorised to serve a 'taxpayer notice' on a UK taxpayer resident overseas to obtain information about that individual's tax position. The Supreme Court in *KBR* distinguished *Jimenez* as being decided on factors not present in *KBR*.

47 'Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime' (3 October 2019), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

© Law Business Research 2021

Home Office, is responsible for incoming MLA requests. Where an incoming request relates to serious or complex fraud, it will be sent directly to the SFO, which is able to use its section 2 powers to assist in obtaining material on behalf of a foreign authority.[48] UK authorities treat incoming MLA requests confidentially. Their practice is to neither confirm nor deny the existence of an MLA request to any third-party enquiry.

Any EIOs received by the United Kingdom after the end of the transition period are now processed as an MLA request.

The FCA and PRA also have the power under section 169 FSMA to assist foreign regulators when requested, including using their coercive powers of investigation.[49] The FCA's guidance confirms that, when deciding whether to use its investigative powers in this way, the FCA will initially consider whether it is able to assist without exercising its formal powers (by getting information voluntarily).[50] However, where this is not possible, in making a decision regarding the exercise of its powers, the FCA may give 'particular weight' to (1) the seriousness of the case, (2) the importance of the case to UK persons, and (3) the public interest. The regulator is not required to investigate the 'genuineness or validity' of a request or to 'second guess a regulator as to its own law and procedures'.[51] In its enforcement policy, the PRA states that it sees providing assistance to overseas authorities as an 'essential part' of the discharge of its functions.[52] Similarly, the FCA Enforcement Guide states that 'the FCA views co-operation with overseas counterparts as an essential part of its regulatory functions'.[53]

11.5.5 US cross-border investigations

US federal and state government agencies commonly share information obtained in an investigation with one another. For example, the DOJ and the SEC are authorised to enforce the FCPA, and they often work together in a coordinated investigation and to bring parallel proceedings.[54] Entities or individuals co-operating with both the DOJ and the SEC in an FCPA matter may be producing information to each agency simultaneously. Further, on

48 To safeguard the privilege against self-incrimination, the SFO requires an undertaking from the requesting authority that any evidence obtained from a person under the SFO's coercive powers will be used against that person in a prosecution.

49 FSMA, s.169(4) sets out the factors the FCA may take into account in deciding whether to exercise its investigative powers.

50 EG 3.7.4.

51 *Financial Services Authority v. Amro* [2010] EWCA Civ 123, a case concerning the FCA's predecessor.

52 Prudential Regulation Authority (PRA), Statement of Policy, 'The PRA's approach to enforcement: statutory statements of policy and procedure' (October 2019), s.6(3).

53 EG 2.6.1.

54 See, e.g., SEC Order, *In the Matter of Walmart Inc.*, File No. 3-19207 (20 June 2019); DOJ Non-Prosecution Agreement, *U.S. v. Walmart* (20 June 2019).

© Law Business Research 2021

22 June 2020, the SEC and the DOJ Antitrust Division signed an MOU to foster co-operation in antitrust matters.[55]

There has been increased coordination among US regulators and non-US regulators. A number of countries, including the United Kingdom, Argentina, Brazil, France, Mexico, South Korea and Vietnam, have enhanced their anti-corruption enforcement laws and are working alongside the United States to investigate and prosecute bribery and corruption.

Therefore, it is important for entities or individuals facing liability in multiple jurisdictions to try to harmonise the substance of data requests where possible. The increasing cross-border nature of investigations underscores the need to consider the impact of privacy laws on data collection, review and productions in each jurisdiction. In addition, the increased sharing of information between regulators can impact decisions as to whether to self-disclose to certain regulators (and the order in which self-disclosures should be made).

Conclusion 11.5.6

Responding to information requests has become increasingly complex as the variety and volume of data has increased, data privacy laws have tightened and regulators are increasingly working together internationally. Dealing with information requests successfully requires adept management of the legal risks in all relevant jurisdictions and careful consideration of how best to advance the position of the company while balancing the cost and business impact of the production.

55 Memorandum of Understanding Between the Antitrust Division, Dep't of Justice and the Sec. and Exch. Comm'n Relative to Cooperation with Respect to Promoting Competitive Conditions in the Securities Industry (22 June 2020), available at https://www.sec.gov/files/ATR-SEC%20MOU-06-22-2020.pdf.

© Law Business Research 2021

12

Production of Information to the Authorities: The In-house Perspective

Femi Thomas, Tapan Debnath and Daniel Igra[1]

12.1 Introduction

Although less common for small and medium-sized enterprises, it is not unusual for large, particularly multinational, companies to find themselves weighing whether to voluntarily disclose information, or what to do when compelled to disclose information to law enforcement or regulatory authorities. The variables to consider are many and nuanced. They include, without limitation, the potential impact on customers and the business, the nature and pervasiveness of the wrongdoing, and whether mandatory reporting obligations arise. This chapter considers some of the key legal and practical considerations implicated when a company produces information to the authorities.

12.2 Initial considerations

The company should seek as early as possible to establish:

- Its status in the inquiry – is it a suspect or witness? This is not always communicated or readily discernible because the authority, itself, might not have decided either way, or might not wish its view to be known in the early stages of an investigation. There may, however, be some clue in how the authority has gone about requesting or otherwise obtaining the information. For instance, in the United Kingdom, a dawn raid by the Serious Fraud Office (SFO) on company premises implies that the SFO, and the courts, have reasonable grounds to believe, based on some assessment of facts, that

1 Femi Thomas is chief compliance officer at Booking.com, Tapan Debnath is head of integrity, regulatory affairs and data privacy – process automation at ABB, and Daniel Igra is legal counsel in Nokia Corporation's ethics and compliance department. The views expressed are the authors' (or as otherwise attributed) and do not represent the views of their employers.

© Law Business Research 2021

it is impracticable to use less intrusive production order powers or doing so creates a risk of destruction of evidence. As such, unannounced raids tend to indicate, though not conclusively, that the company is a suspect.[2]

- Are any of the company's employees suspects, and do they pose any ongoing risks to the business?[3] When employees are suspects, a company should ensure that data collection and any internal investigation is conducted without tipping off the implicated employees or 'trampling over the crime scene', while adhering to local data protection and labour law. Depending on the jurisdiction and the authority involved, the company may need to disclose to the investigating agency that it intends to seek information from company employees. This may help to avoid inadvertent and unwanted interference with the agency's own activities.[4]
- Which authority is making the request, and is the request reasonable? Some authorities are more aggressive than others; this is worth factoring in when setting the response strategy. Equally important is determining whether there are multiple authorities involved. Requests from less familiar jurisdictions, where the independence of prosecutors and the judiciary might be less assured, pose additional questions: Is there a political or monetary motivation? Are employees at risk of arrest and imprisonment without adequate due process? And what are the rules of corporate liability, if any? A request for information should be carefully reviewed to ensure that it appears reasonable in terms of scope and the basis for the request, and that it states the power under which the request was made.

Data collection and review 12.3

The company will at an early stage start to think about whether it has the responsive data and the appropriate process for preserving and collecting it. Data from digital devices to be produced to the authorities should be safeguarded from deletion or destruction and then collected in a forensically sound way. At a high level, this means that the collection is carried out by skilled

2 On 6 August 2019, the SFO published its long-awaited Corporate Co-operation Guidance. At the end of the Guidance, a short passage explains that it may be necessary for the SFO to exercise powers of compulsion to obtain material from a co-operating company. This re-enforces that how the authority seeks material (whether by production order or dawn raid) can be illustrative only of the company's status in the investigation and should not be taken as conclusive.

3 While change of company personnel (and culture) is a desirable outcome in most cases involving serious wrongdoing, it will probably need to be considered after a thorough review of the issues.

4 Agencies such as the US Department of Justice (DOJ) and SFO have considerable powers to sanction non-compliance with requests for information. While such sanctions have been seldom used in the United Kingdom, the SFO did secure its first conviction after trial in January 2020 in relation to its ongoing *ENRC* investigation for failing to comply with a notice pursuant to s.2 of the Criminal Justice Act 1997.

© Law Business Research 2021

persons who can retrieve and preserve whole images of various types of devices in a manner that is repeatable with consistent results, and that all steps taken are recorded and auditable. It is vital to capture all relevant material, and having a systematic and methodical approach will help. The investigation support team should include someone with detailed knowledge of the company's IT systems and structure and will, preferably, be experienced in data extractions.

A company is also likely to want to understand for itself what the collected data reveals. The data review is invariably the most time-consuming and costly part of the production exercise. It is therefore imperative to try to agree realistic deadlines with the authorities at the outset and to communicate promptly if any slippage is anticipated. Most authorities will want a written record, usually in the form of witness statements, of the methodology used in the data collection and imaging, the process and rationale behind any filtering of the data, and how the review was conducted and the instructions given to the reviewers. This point is stated explicitly in the Corporate Co-operation Guidance published by the SFO on 6 August 2019 under the heading 'Preserving and providing material'. The SFO Guidance emphasises the need to have an audit trail of the acquisition and handling of digital material and to take all steps to maintain the integrity of systems hosting such material over the life of an SFO investigation, which can run for many years.

A corporate can manage the costs incurred in a data collection and production exercise by: having an established panel of specialist law firms, which should yield discounted rates, but maintaining flexibility to go off-panel as individual case needs dictate; outsourcing the data collection and document review to professional service providers or even doing it in-house[5] if there is the requisite capability; ensuring that the document review is as focused as possible through appropriate filtering and, possibly, use of AI technology; setting a budget at the outset and sticking to it unless extensions are approved; and monitoring costs on a monthly basis to ensure the exercise remains within budget. In an about-face from the wave of outsourcing that predominated in the past decade or so, large corporates are increasingly building in-house e-discovery proficiencies. A well-resourced programme need not be burdensome, but will pay dividends at production time by sharply reducing some of the larger-ticket items in document production – data collection, processing and culling (coordinated, as necessary, jointly with outside counsel).

12.4 Principal concerns for corporates contemplating production

There are numerous, often competing, concerns when a company produces documents to the authorities. One obvious but important concern is the impact that the disclosed material might have on (1) the authority's investigation, or

5 Some companies have an in-sourced legal support function that handles, for example, initial review of contract terms, which can, with some training and guidance, be used to do the first document review in an internal investigation.

© Law Business Research 2021

even pre-investigation, and (2) the company's status with the authority. Another concern is the ability to identify and protect any intellectual property, trade secrets or proprietary information, or commercially sensitive information that might be contained in, or decipherable from, the material to be disclosed. This concern will accentuate when the company is co-operating with authorities in a cross-border context, or where multiple authorities have taken, or could take, an interest. The disclosed material could end up being shared between the various authorities, which could result in disparate recognition or application across different jurisdictions of limitations on use (as provided under statute or as agreed with one authority). As a result, the disclosing party cannot necessarily ensure that the limitations on use – which applied in the jurisdiction in which the material had been disclosed – will be enforced in a separate jurisdiction in which the material is now available.[6]

Relatedly, the corporate will be interested in preserving protections afforded under the attorney-client privilege or its jurisdictional equivalents. Special care must be taken at the start and throughout the investigation to have clear records of who is authorised on behalf of the company to instruct and receive advice from external lawyers, and is therefore the client. The purpose of any internal investigation is important also and should be recorded. Is the purpose to obtain legal advice on the company's position in relation to a law enforcement or regulatory authority's interest? Is it to gather information to disclose to the authorities? Or is it to do with actual or contemplated litigation, or a combination of reasons?

With the Court of Appeal ruling in *SFO v. ENRC*,[7] it is now easier for corporates to argue successfully that litigation privilege applies to certain parts of its internal investigation, including over employee and third-party interviews and material generated by forensic accountants. While the question of who is the 'client' remains narrowly construed, namely those who have been authorised by the company to instruct and receive advice from lawyers, the Court of Appeal expressed a non-binding view that the law in this area could be reviewed and updated.[8] For now, it remains more difficult to apply legal advice privilege to the fact-gathering part of an internal investigation.

See Chapter 36 on privilege

6 In *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017), the US Court of Appeal overturned the convictions and indictments of two LIBOR traders because, among other things, the testimony given by the defendants to the UK Financial Conduct Authority (FCA) under compulsion was used against them in their US criminal trial, which was held to be an infringement of the defendants' Fifth Amendment rights. This is an example of information given in one jurisdiction (the United Kingdom), in which there were statutory limitations on use of the information, being used without limitation, initially at least, by another (the United States).

7 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2018] EWCA Civ 2006.

8 The Court of Appeal in *Civil Aviation Authority v. R (on behalf of the application of Jet2.com Ltd)* [2020] EWCA Civ 35 also indicated that it does not believe that this principle should be the law, but that it remains the law, unless the Supreme Court intervenes.

© Law Business Research 2021

A company will also be keen to restrict the ability of third parties to use the information disclosed to the authorities in civil proceedings against the company. Such restrictions could be imposed during the course of negotiations or discussions aimed at resolving, avoiding or reducing the scope of litigation by making clear at the time of production that the information is confidential and, when dealing with UK authorities, stated to be provided on a limited waiver of legal privilege or without-prejudice privilege basis.[9] A company contemplating this approach should keep in mind that it loses control over material that has been disclosed to authorities. The material might, for example, via court orders for disclosure, end up in the hands of litigants, regardless of attempts to prevent it. Second, the attempt to make the disclosure of material without prejudice to privilege could clash with the authority's expectation of a co-operating entity and negatively affect the chances of non-prosecution. This is particularly the case in view of a 2018 judicial review in which the High Court criticised the SFO and re-emphasised the SFO's obligation to proactively seek to obtain material that might help the case of individual defendants or undermine the prosecution's case, even if that means testing and challenging a company's assertion of privilege over the product of an internal investigation.[10]

Federal courts in the United States are reluctant, however, to recognise selected waivers of privilege in relation to documents produced as part of an investigation or prosecution.[11] The information may lose the protection of privilege and be subject to discovery by other parties.

See Chapter 37 on privilege

It is also noteworthy that legal privilege in most European countries is generally treated somewhat differently than it is in the United Kingdom and United States. France and Germany, for example, apply the doctrine of professional secrecy or confidentiality of communication between the client and his or her attorney. Lawyer–client communications are, pursuant to the doctrine, protected from disclosure to external parties, subject to the crime exception. The status of any material created by lawyers during an internal investigation will need to be carefully considered. This is especially so because material created by in-house counsel conducting an internal investigation not under the auspices of an external lawyer-led investigation, is unlikely to attract the professional secrecy or confidentiality protection.

Adherence to data protection principles is another important concern, especially when the information is being provided to the authority voluntarily and there is consequently not the protection given by a document production order or subpoena, which usually overrides any local data protection rules. Since 25 May 2018, Article 48 of the EU General Data Protection Regulation

9 *Property Alliance Group Ltd v. Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch) without prejudice privilege applied to negotiations with the FCA with a view to arriving at a settlement. The without prejudice rule applies to exclude negotiations genuinely aimed at settlement from being given in evidence.

10 See *R (on the application of AL) v. Serious Fraud Office* [2018] EWHC 856.

11 See *In Re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289 (6th Cir. 2002).

© Law Business Research 2021

(GDPR) has restricted the ability of companies to transfer information out of the European Union in order to respond to orders or requests of foreign courts or authorities. Under this Article, personal data can only be transferred outside the European Union to respond to law enforcement or regulatory subpoenas or production orders, or court orders for disclosure, through the mutual legal assistance treaty route or other provisions of the GDPR. As the application of Article 48 is yet to be examined by the courts, it is unclear whether voluntary disclosure to the authorities is caught by the Article.[12]

Obtaining material from employees 12.5

There will often be a wide pool of employees, a few of whom might be 'suspects' or 'targets', who hold relevant information. It is important to first identify which, if any, of those employees should be notified of the data collection, bearing in mind the SFO cautioning against putting employees on notice and its desire to have the data collection undertaken with minimal risk of interference.[13] The Corporate Co-operation Guidance states that the SFO should be consulted before interviewing employees (or taking any HR action). When collecting data from employees, the corporation should be mindful of local laws and the company's policies on data collection, as well the potential need to give notice or obtain consent from the employee. The key is to weigh any risk of relevant information being destroyed, and displeasing the requesting authority, if notice of the data collection is given to employees against any specific local law requirements and internal data collection policies.

It is common for employees to have personal material on work devices. If there are no reasonable grounds to believe that giving notice of a data collection exercise to an employee creates a risk that data will be destroyed, the employee could be instructed to separate personal material from work material before the device is copied. The personal material would then be safe from inadvertent disclosure to the authorities. If this separation of personal data is not possible because, for instance, the collection needs to be covert, then filtering and review before disclosure, if appropriate, should provide adequate safeguards against personal data being handed over.

A growing trend is for work material to be stored on personal devices. The covid-19 pandemic has prompted an explosion in the number of people working from home, increasing the use of own devices, which many companies permit through BYOD (bring your own device) polices. If that same material also exists on a work device or on the company's servers, it can be collected from there rather than from the employee's personal device. Clearly, it is not

12 See, for example, David J Kessler et al., 'The Potential Impact of Article 48 on Cross Border Discovery From the United States' in *The Sedona Conference Journal*, Volume 17, 2016, No. 2.

13 Speech by Alun Milford, SFO General Counsel, Annual Employed Bar Conference, 26 March 2014, available at https://www.sfo.gov.uk/2014/03/26/corporate-criminal-liability-deferred-prosecution-agreements/.

© Law Business Research 2021

permissible for a company to covertly extract data from an employee's personal device but it may be possible to do so with the employee's express consent. Such situations should be catered for in the contract of employment and the company's internal policies.

Another effect of the pandemic is that working from home or hybrid working is becoming the norm. This may mean that employee-created paper notes and other hard-copy material that had previously been kept in office locations are now being stored at employees' home addresses. It should be noted that employees' country of work may have changed due to the pandemic. For instance, employees may have returned to their home country from their country of assignment during the pandemic. The movement of material stored on devices and elsewhere from one country to another may impede the company's access to that material for specific purposes. For example, material transferred to France by an employee previously working in the United States may be caught by the Blocking Statue should the company require that material for US litigation or to produce to US authorities. Likewise, that material becomes more readily accessible to the French authorities if required for their inquiries. Companies will do well to map out such risks as they craft their remote working policies.

As a best practice, companies should guard against this thorny issue of commingling of personal and business information by instituting appropriately tailored policies. It may not, however, be reasonable to expect that a company device will never be used for some personal purposes but companies should provide written limitations on the kinds of use that are acceptable and permitted. In any event, the transfer of business data through personal devices or personal email accounts should always be governed by appropriate mobile phone and BYOD policies. The policies should require, by way of non-exhaustive examples, line manager approval; only recommended devices be used; and only corporate subscription is permissible, which means that the device is linked to and can be controlled through the company's systems. .

The foregoing considerations are further complicated by the increasing popularity of social media platforms, such as WhatsApp, text messages and iMessage, which are expensive and difficult – if not impossible – to recover once deleted, in corporate communications. Companies increasingly must preserve (and produce) business communications made via ephemeral messaging apps (EMAs), which fall broadly into two categories: 'popular social media', WhatsApp and so forth; and business messaging platforms, such as Slack, Yammer and Workplace. The distinction between the two is important because popular social media platforms are more likely to have more private than business data than the business platforms. The retrieval of business data co-mingled with 'private' data is much more complex and burdensome, especially in countries with strict data protection laws, if not generally impermissible without the employee's express and freely given consent. Companies should continue to exercise vigilance over business use of EMAs – including business messaging platforms; provide centrally hosted and backed up messaging for

© Law Business Research 2021

business communications and sensible social media use policies; understand server data locations for each service (particularly those used by the business as opposed to those used by individual employees); and put in place data retention policies to ensure clarity around what sort of data is preserved and for how long. US and UK authorities expect companies to be able to retrieve EMAs in an investigation.

Material held overseas 12.6

Because of the global nature of business, information that is required by a law enforcement or regulatory authority might be held by the company's overseas subsidiaries – and in multiple locations at that.

When a company seeks to provide information voluntarily, it should assess whether this would expose it to potential claims of breaching the confidentiality or data protection rights of employees or third parties.

Despite a company's desire to co-operate with a subpoena or production order, there may be significant legal hurdles, such as blocking statutes, preventing it from providing the material.[14] There have been several US and UK court decisions[15] that, applying the 'law of the forum' principle, ruled that the risk of prosecution for breaching an overseas blocking statute is not a reasonable ground for non-compliance with the court's order for discovery. In those circumstances, the company's lawyers must speak with the authority concerned, explain the issues and diplomatically suggest that the authority consider obtaining the information through the MLAT route or through police-to-police information exchange. It is vital for the company to support the process by having the material readily available, and using the contacts that the company's external lawyers might have with prosecutors in the state where the material is held, to try to expedite matters. A legitimate alternative is available if the information also exists independently in another jurisdiction, which does not have blocking statutes, provided it had been transferred there previously for valid business or legal purposes and not to get around the blocking statute.

There have been recent important legislative developments in the United States and United Kingdom that seek to make it easier for law enforcement

14 France, Switzerland, Italy and China are some of the countries that have blocking statutes. Breach of the Swiss blocking statute has been prosecuted on several occasions, whereas breach of the French blocking statute has, as far as is known, been prosecuted only once since its inception in 1968. However, Sapin II has a provision for penalising breach of the French blocking statute, which leads some commentators to believe that it will be more readily enforced. Further, Article 48 of the EU General Data Protection Regulation has similar effect to blocking statutes across the European Union. (See, further, Vol. II chapters at question 61.)

15 For example, *Secretary of State for Health and Others v Servier Laboratories and Others (Servier)* [2013] EWCA Civ 1234 and *National Grid Electricity Transmissions PLC v ABB Limited and Others* [2013] EWHC 822 (Ch).

© Law Business Research 2021

to access electronic data held overseas. The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and the UK's Crime (Overseas Production Orders) Act (COPO Act) 2019 allow the authorities to compel companies, without having to apply to a court, to hand over information even where the information is held overseas. The UK–US Bilateral Data Access Agreement, signed on 3 October 2019, will lead to prosecutors gaining these additional powers.[16] These are the first acts of the kind and reflect the theme of increased cross-border co-operation. While the impact of the legislation remains to be seen, the acts clearly represent another point at which companies can be caught between conflicting laws, with blocking statutes and data privacy laws at the other side of the pincer seeking to limit companies' ability to provide information. Companies should therefore be acutely aware of the potential for such conflicting obligations, and understand who controls their data (third parties may host or store data) and where it is stored. It is also prudent to develop plans of action for how to respond to an order to furnish evidence kept in a jurisdiction with laws prohibiting the transfer.

The February 2021 decision of the UK Supreme Court in *KBR v. SFO*[17] allowed an appeal against a High Court ruling which deemed that a non-UK registered company could be compelled under section 2 of the Criminal Justice Act 1987 to produce to the SFO material held overseas provided there was a sufficient connection between the company and the United Kingdom. In this case, KBR Inc, organised in the US, was issued with a section 2 notice for material held overseas in connection with an SFO investigation into KBR Inc's UK subsidiary. The Supreme Court overturned the High Court decision on the basis that it had not been the intention of Parliament to give the SFO such extraterritorial powers, noting that Parliament had instead developed MLA to facilitate gathering of material held internationally.

12.7 Concluding remarks

As explained in Chapter 11, there are many good reasons why a company might wish to take a proactive approach and voluntarily provide information rather than waiting for a subpoena or production order. It could, for example, give the best opportunity for maximising co-operation credit. The senior English judge granting the Rolls-Royce deferred prosecution agreement (DPA) cited voluntary provision of material as one of the ways Rolls-Royce demonstrated 'extraordinary' co-operation. This was also highlighted as a key element of Airbus's co-operation, which led to DPAs with the SFO and US Department

16 The Agreement came into force on 8 July 2020.

17 *R (on the application of KBR, Inc) v Director of the Serious Fraud Office* [2021] UKSC 2

© Law Business Research 2021

of Justice and an equivalent *convention judiciaire d'intérêt public* (equivalent to a DPA) with France's Parquet National Financier in January 2020.[18]

From a US perspective, the DOJ expressly encourages corporates to co-operate with their investigations. For example, the second edition iteration of the DOJ and SEC Resource Guide to the US Foreign Corrupt Practices Act[19] emphasises that corporates enjoys most favourable treatment under the April 2020 Corporate Enforcement Policy by demonstrating full and timely co-operation, together with self-disclosure, a comprehensive internal investigation, willingness to pay disgorgement, and an enhanced and effective compliance programme.

Depending on the facts of the case, in the authors' view, there could be little to no loss of credit by asking for a production order rather than voluntarily disclosing – if this is appropriate to overcome data protection or other barriers – provided (1) there is early dialogue with the authorities and (2) the issues are reported before the authority learns of them separately through another source.[20]

In some circumstances a company might wish to think carefully about whether it needs to demonstrate extraordinary levels of co-operation. One way to do so would be to waive legal privilege over certain classes of documents to influence the company's eligibility for the United States Department of Justice's FCPA Corporate Enforcement Policy[21] or a DPA.[22] The joint Crown Prosecution Service and SFO Guidance on Corporate Prosecutions[23] explains that 'genuinely proactive' self-reporting is a public interest factor militating against the prosecution of a company. A voluntary waiver of privilege is relevant to determining whether a company has genuinely and proactively co-operated with the SFO or other authority, and consequently to the assessment of whether it is in the public interest to prosecute or to invite the company to DPA negotiations. The SFO Corporate Co-operation Guidance states that a failure to waive privilege and provide witness accounts will not allow the company to avail itself of the corresponding factor weighing against prosecu-

18 *United States of America v. Airbus SE*, Case No. 1:20-cr-00021, Convention Judiciaire Intérêt Public between the Parquet National Financier and Airbus SE [2020] (PNF-16 159 000 839); *Director of the Serious Fraud Office v. Airbus SE* [2020] Case No. U20200108.

19 Published on 2 July 2020.

20 Rolls-Royce did not self-report but still received a deferred prosecution agreement because of its 'extraordinary' co-operation. See *Serious Fraud Office v. Rolls-Royce plc and another*, Case No. U20170036 (2017), paras. 21, 22.

21 The Corporate Enforcement Policy adapted and replaced the FCPA Pilot Program – see https://www.justice.gov/criminal-fraud/corporate-enforcement-policy. The policy includes a presumption of a declination where the company voluntarily self-reports, fully co-operates with a DOJ investigation and makes timely and appropriate remediation.

22 Of course, the implications of full or selective waiver of privilege must be very carefully thought through.

23 Available at https://www.cps.gov.uk/legal-guidance/corporate-prosecutions.

© Law Business Research 2021

tion as found in the SFO and CPS Deferred Prosecution Agreements Code of Practice[24] (but will not be penalised by the SFO). In France, Guidelines on the Implementation of the Convention Judiciaire d'Intérêt Public[25] make clear that an assertion of legal privilege that is deemed by the prosecutor to be unjustified has an 'unfavourable effect on the level of cooperation of the company'. The Guidelines do add, however, that the risks companies may face in other jurisdictions by waiving privilege will be taken into account. Considering current policy in the United States, United Kingdom and France, a company might wish to think carefully about which documents it believes are truly legally privileged and whether in fact to assert legal privilege over them.

As stated in opening this chapter, there are many and nuanced factors to consider when a company is required to produce information to the authorities. The key is to be well prepared in terms of knowing where information is stored; to have the relevant expertise, preferably internally, to gather relevant information quickly and forensically; to have an overall strategy and end game as early in the process as possible, but also keeping things under review; and to be able to rely on trusted advisers.

24 Available at https://www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf.

25 Available in English at https://www.agence-francaise-anticorruption.gouv.fr/files/files/EN_Lignes_directrices_CJIP_revAFA%20Final%20(002).pdf.

© Law Business Research 2021

13

Employee Rights: The UK Perspective

James Carlton, Sona Ganatra and David Murphy[1]

Contractual and statutory employee rights **13.1**
Company policy, manual, contracts, by-laws **13.1.1**
Suspension 13.1.1.1

The vast majority of employees implicated in an investigation will be suspended. Usually, employers will rely on the increasingly common express provisions to suspend employees in the course of disciplinary investigations contained in the employment contract, staff handbook or disciplinary policies.

In the absence of such an express provision, employers may still suspend employees on the basis that it constitutes a reasonable management instruction not to work or attend the workplace in circumstances where serious allegations, particularly those of a regulatory nature, have been made or where relationships have broken down.

In such circumstances, however, employees may have greater grounds to challenge the suspension. English case law in relation to garden leave (when an employer requires an employee not to attend work during the notice period) suggests that if the employer does not have an express right to suspend an employee, the employee may have a legal basis for challenging the suspension if he or she can show that he or she needs to be able to use particular professional skills frequently to ensure that they are maintained and do not diminish through lack of use.[2] Even if the employee cannot show this, the longer the period of suspension, the more difficult it may become for the employer to justify it.

1 James Carlton, Sona Ganatra and David Murphy are partners at Fox Williams LLP.

2 *William Hill Organisation Limited v. Tucker* [1998] IRLR 313.

© Law Business Research 2021

Regardless of whether it has relied on an express right or not, employers must have reasonable grounds for any suspension and these grounds should be kept under review to ensure that the period of suspension is no longer than necessary.

13.1.1.2 What constitutes a reasonable ground for suspension?

Suspension may be reasonable if the individual is suspected of serious misconduct and his or her continued attendance at work creates a potential threat to the employer's business or its other staff or could have an adverse effect on the investigator's ability to investigate the matter appropriately. In the event of a legal challenge to suspension, an employment tribunal or court is likely to consider all the relevant circumstances, including the terms of the employee's contract, what the employer has said about the suspension, the length of suspension and any financial loss it is causing. The courts have held that the only test that must be satisfied by an employer is that it had 'reasonable and proper cause' to suspend the individual. The employer need not show that suspension was necessary.[3]

Most employers' disciplinary procedures are not contractual, and therefore a failure to follow them does not, generally speaking, constitute a breach of contract (unless the employee can show that the failure was a breach of the implied duty of trust and confidence owed by the employer). However, in the public sector, where contractual procedures are more common, there have been circumstances in which employees have successfully obtained injunctions preventing their employers from proceeding with disciplinary proceedings where to do so in the particular circumstances would constitute a breach of contract.[4]

Given the potential for disciplinary action to have significant adverse consequences on the careers and finances of employees working in regulated sectors, in the coming years we may see employees pursuing creative legal arguments to obtain injunctions against disciplinary action. Such arguments might be based on the implied duty of trust and confidence, with employees arguing that proceeding with disciplinary action in the particular circumstances would breach the duty.

In the United Kingdom, the statutory Code of Practice on Disciplinary and Grievance Procedures (the Code) published by the Advisory, Conciliation and Advisory Service[5] sets out the principles for handling disciplinary and grievance issues in the workplace. Its content in relation to investigations is written with internal investigations in mind, rather than investigations by an external third party, but its principles will be relevant to any disciplinary proceedings instigated by the employer and therefore to all investigations that might lead to disciplinary action. Individuals will not have any free-standing claim for any

3 *London Borough of Lambeth v. Agoreyo* [2019] EWCA Civ 322.

4 *Mezey v. South West London & St George's Mental Health NHS Trust* [2010] IRLR 512.

5 https://www.acas.org.uk/acas-code-of-practice-for-disciplinary-and-grievance-procedures/html.

© Law Business Research 2021

failure to follow the Code but employment tribunals take into account any such failures when considering relevant cases and the compensation to be awarded.

In practice, in a regulated environment such as the financial services sector, many employers will be far less concerned about compliance with the Code than they will be about satisfying the demands and wishes of the regulators or prosecuting authorities. Nonetheless, an individual who does not consider an investigation is being handled appropriately may find within the Code's principles some helpful points to refer to when explaining his or her concerns to the employer. In particular, that any period of suspension should be kept as brief as possible and should be kept under review.

Remuneration 13.1.1.3

It is usual for employees to continue to receive basic salary and benefits while an investigation is ongoing, irrespective of whether they are suspended from work. Unpaid suspension is rare and will not usually be an option open to the employer unless it has a contractual right to do so.[6]

In the financial services sector, variable pay (such as annual bonuses and long-term incentive awards) often forms a significant part of an employee's annual remuneration and normally a proportion of variable pay is deferred and paid out over a number of years.

It is now common to see provisions in employment contracts to the effect that variable pay will not be awarded or delivered if at the time of award or delivery the individual is subject to any kind of investigation. Similar provisions are usually also found within the relevant award plan rules.

Investigations can take many years so their implementation can have a significant financial impact on the employee, particularly as it can affect deferred remuneration from prior years, as well as the current year's bonus or long-term incentive scheme award.

It is not always clear from such provisions what happens to any variable pay that is not awarded or delivered if the investigation finds there has been no wrongdoing. When negotiating employment contracts, employees should seek clarity in the wording of the provisions so they stipulate that if an investigation finds no wrongdoing, the variable pay in question be awarded or delivered.

In relation to variable remuneration awarded by banks, building societies and certain regulated investment firms, the regulatory framework contains strict restrictions for particular classes of employees.[7]

In essence, the rules are intended to discourage excessive risk-taking and encourage more effective risk management.

---

6 *North West Anglia NHS Foundation Trust v. Gregg* [2019] EWCA Civ 387.

7 As set out, for example, in SYSC 19D of the Financial Conduct Authority (FCA) Handbook in respect of dual regulated firms: https://www.handbook.fca.org.uk/handbook/SYSC/19D/?view=chapter.

© Law Business Research 2021

By way of illustration, the rules provide that, in certain circumstances, deferral (the period during which variable remuneration is withheld following the end of the accrual period) is extended to (1) a minimum seven-year period with no vesting until three years after award for senior managers (i.e., individuals who have the greatest influence over the strategic direction of the business), (2) five years for Prudential Regulatory Authority (PRA) designated risk managers with senior, managerial or supervisory roles, and (3) three to five years for all other staff whose actions could have a material impact on a firm (material risk-takers).

At the same time, dual-regulated firms[8] must include *malus* provisions (i.e., arrangements that permit the employer to prevent vesting of all or part of deferred remuneration based on risk outcomes or performance) and clawback provisions (i.e., arrangements through which remuneration that has already vested is recouped) for seven years from the award of variable remuneration for all material risk-takers. Importantly, both the PRA and the Financial Conduct Authority (FCA) clawback rules have been strengthened by a requirement for a possible three additional years for senior managers at the end of the seven-year period where a firm or regulatory authorities have commenced enquiries into potential material failures. In effect, therefore, employees operating at a senior level in the financial services sector who are subject to an investigation potentially now face a decade of uncertainty over their pay.

Guidance from the FCA provides that, in relation to issues relating to risk-management failure or misconduct, regulated firms are expected to consider cancelling or clawing back bonus awards in relation to those employees who reasonably could have been expected to be aware of the failure, misconduct or weakness at the time but failed to take 'adequate steps' or who, by virtue of their role or seniority, were 'indirectly responsible or accountable'.[9]

A key related issue is the operation of these *malus* or clawback provisions in the context of the buy-out of awards when an employee moves from one firm to another. As a result of the regulatory framework, senior employees in the financial services sector may find that their current employer is able to apply clawback based upon the conclusions of their previous employer's investigation. As such those employees who are subject to an investigation in the regulated sector can face further uncertainty and the possibility that previous employers can determine their future pay.

13.1.2 English law

Suspended employees are bound by the express terms of their contracts and by certain terms implied by law, including a duty of fidelity (which includes a duty of confidentiality) and a duty to obey lawful and reasonable orders.

8 A 'bank, a building society or a UK designated investment firm', FCA Handbook, SYSC 19 D.

9 https://www.fca.org.uk/publication/finalised-guidance/guidance-on-ex-post-risk-adjustment-variable-remuneration.pdf.

© Law Business Research 2021

At the same time, employers are also bound by an implied duty of trust and confidence. This duty comes into play when determining whether to suspend employees implicated in misconduct.

Employees have successfully argued that a failure to consider whether suspension could be avoided was a breach of the duty of trust and confidence owed by the employer in numerous cases, paving the way for a claim for constructive dismissal.[10] Such claims are often difficult to pursue but, if successful, release the individual from any post-termination restrictions in his or her contract. Accordingly, prudent employers should keep under continuous review the need for an employee to be suspended.

Representation 13.2

Need to collect information on behalf of client 13.2.1

Interviewing client 13.2.1.1

At the outset of an instruction from an individual, independent legal advisers (ILAs) should seek detailed instructions to determine the potential scope of the misconduct under investigation and the parties implicated. A key component of this stage is to assess the employee's relationship with the employer. Understanding the dynamics of the relationship at the outset will assist in the smooth running of the investigation and allow a better understanding of the support that is likely to be offered by the employer.

Requesting documents and information from: 13.2.1.2

Employer

An employee involved in an investigation (internal or external) may need to request that the employer provides documentation, access to witnesses or other support. During any period of suspension, the individual is often operating in a vacuum, and he or she is likely to be prohibited from having contact with clients and colleagues and prevented from having access to the employer's IT systems, documents and premises other than to the extent permitted by the employer. There is unlikely to be an express or implied right that the employee can rely on support from the employer.

From an employer's perspective these restrictions are crucial to ensuring that documentation has not been compromised and that potential witnesses or accomplices have not been tipped off. Indeed, such concerns may also be important for the employee.

In the context of an internal investigation, the employer would not want to provide carte blanche access to documentation and information to the employee and is likely to prefer that the employee provide his or her own account of the circumstances.

10 For example *Crawford and another v. Suffolk Mental Health Partnership NHS Trust* [2012] IRLR 402.

© Law Business Research 2021

In the context of an external investigation by law enforcement authorities, the situation is more complex. It may well be in the employer's interests to co-operate with requests for assistance to gain some understanding as to the scope of the investigation and the potential repercussions. At the same time, the employer may have its own regulatory obligations in mind and may be required to co-operate with and disclose documentation to the regulator.

Any rights of the employer to access the content of personal electronic devices used by the employee for work are likely to be set out in the staff handbook. In general, where such devices are routinely used for work purposes, employers will be permitted to seek access to them.

Law enforcement

In circumstances where a law enforcement authority has announced its intention to interview an individual, a request for a list of questions or topics of discussion together with relevant documentation should be made to the relevant body at the earliest opportunity. In practice, law enforcement authorities seldom provide more than a broad list of areas they wish to explore and often provide limited supporting documentation. Individuals should be advised at the outset that they are unlikely to receive detailed information from the law enforcement authority in advance of the interview and that further documentation is likely to be produced on the day of the interviews. There will be specific, limited circumstances, however, where law enforcement authorities are more receptive to such requests. For example, if the individual is no longer in employment and has no ongoing relationship with the employer or if the employer is no longer operating as a going concern, law enforcement authorities may be more amenable to requests for information as otherwise the employee will have no other avenue to properly prepare a case.

Other witnesses (and their counsel)

As noted above, individuals are likely to be prohibited from having contact with clients and colleagues during suspension. If an individual is aware of colleagues who can provide assistance to clarify aspects of the case, appropriate action should be taken to contact them. Depending upon the ongoing relationship with the employer, in the first instance, it may be sensible to approach the employer to request details of the colleague's legal counsel (if one has been appointed).

13.2.2 Joint defence agreements

13.2.2.1 Between individuals and the company

In the vast majority of circumstances, co-operation between the employee and employer will be mutually beneficial. From an individual's perspective, while there is a risk of self-incrimination, co-operation with the employer allows the employee to understand how the investigation is progressing and whether external regulators are involved, and have a greater chance of accessing

© Law Business Research 2021

materials that are relevant. Such co-operation often results in work-product produced by and communications between the parties and their legal advisers being protected by common interest privilege.

While perhaps not as frequent as in the United States, settlement discussions with law enforcement authorities in the United Kingdom are a growing trend in fraud and corruption matters. At the time of writing, since the introduction of deferred prosecution agreements (DPAs) in 2014,[11] the SFO has entered into 12 DPAs. These agreements are not currently available for individuals in the United Kingdom. ILAs should ensure their clients appreciate the risk that the law enforcement authority may still take action against the employee in circumstances where the employer has entered into a DPA. Interestingly however, recent cases have shown that in circumstances where the corporate has entered into a DPA, the SFO has struggled to prosecute employees for the same alleged misconduct.

Between individuals and their counsel 13.2.2.2

In complex cases of misconduct, there are likely to be a number of individuals involved. There are clear advantages to ensuring communication lines are opened and maintained with ILAs engaged by potential 'co-defendants'; such communications have the benefit of being protected by common interest privilege. The many advantages include the sharing of important information and documentation that others may have obtained, as well as the benefit of adopting a common approach with the employer to documentation requests. Employers are more likely to be receptive to common, and therefore more focused, information requests made by several employees rather than numerous different requests received at different times by each employee.

Indemnification and insurance coverage 13.3

Determining whether an individual is indemnified 13.3.1

Upon instruction by an individual, clarification should be sought as to whether the employer will fund the costs of an ILA. From the employee's perspective, access to an ILA from the start of an investigation is essential (regardless of whether the employee is central to the allegations or on the periphery) given the potential dangers ahead. What may start off as the provision of an innocuous witness account to a regulatory authority may turn quickly into the employee being regarded as a suspect as new allegations of misfeasance surface.

11 Schedule 17 of the Crime and Courts Act 2013, which allows the Director of the Serious Fraud Office (SFO) and the Director of Public Prosecutions, and other prosecutors designated by the Secretary of State, to enter into DPAs.

© Law Business Research 2021

13.3.1.1 Employment contract, company policies, by-laws or local laws

It is unusual to see rights of indemnification set out formally in employment contracts in the United Kingdom. Unlike other jurisdictions, English law does not provide indemnification rights to employees.

In certain industries, however – for example, the financial services and media sectors – it is becoming increasingly common for employers to maintain formal policies setting out the circumstances in which they will indemnify employees' legal expenses. Such indemnification will be limited to situations where an employee is being investigated solely because of acts performed in the course of and within the scope of his or her employment.

Close attention should be paid to such policies and the restrictions set out in them. In particular, given the difficulties for an employer to determine the potential liability of an employee at the outset of an investigation, it is common for employers to provide indemnification for legal fees incurred at an initial stage while the scope of allegations is clarified and for the employer to have a right to stop further indemnification and seek reimbursement of earlier costs, for example, where the employee is found to have acted outside the scope of his or her employment.

Employers also, generally speaking, provide lists of approved law firms to act as ILAs and generally require employees to seek approval before appointing representatives not on the list.

13.3.1.2 Insurance policies of employer

Employees at a senior level may also benefit from directors' and officers' (D&O) insurance.

The coverage of D&O policies should be carefully considered from both the employee's and employer's perspective to ensure that the policy covers investigations, prosecutions and related civil claims.

In general, UK-based D&O policies provide cover for 'formal' investigations. ILAs should clarify whether the definition of investigations also includes internal investigations and consider whether other policies may be relevant. If an internal investigation has been commenced by the employer, for example, as a result of concerns over its own conduct and liability, other insurance policies, such as professional indemnity insurance, might be engaged. At the same time, the D&O policy might include an exclusion in relation to claims in connection with the performance or failure to perform professional services by or on behalf of any director or officer. In such circumstances, the professional indemnity insurance policy should become engaged. The exclusion of the D&O insurance and application of professional indemnity (or other related) insurance is frequently debated at the outset of investigations, particularly where there is concern about the requirement to pay deductibles under the D&O policy or where there are local insurance requirements under a global policy.

© Law Business Research 2021

Advocating for indemnification when not otherwise clear 13.3.2

From the employer's perspective, the appointment and funding of an ILA has clear benefits where it appears that the interests of both parties are congruent. It encourages the co-operation of the employee and assists in ensuring that certain communications with the employee can be made with the protection of privilege.

See Section 13.4

While indemnification policies are becoming more common, many employers choose not to have a formal policy and instead seek to enter into separate arrangements at the time of the investigation. This approach is attractive from the employer's perspective as it enables the employer to select when and how it will indemnify certain individuals without setting a precedent. In such circumstances, the employee should negotiate carefully to ensure that all potential costs and eventualities are covered.

Awareness of situations where indemnification may cease 13.3.3

Violation of undertaking to the company 13.3.3.1

Employer policies will set out the circumstances in which indemnification will cease. A common provision is the employee acting contrary to restrictions and requests set out in the agreement. For example, the indemnification policy or agreement may contain clauses requiring the employee to act in good faith in its dealings with the employer and regulatory authorities or to provide updates to the employer at given stages. Such undertakings should be highlighted in advance to individuals and ILAs should ensure that information is provided to the employer and its counsel.

It is important to advise individuals at the outset that violation of certain provisions may also lead to the employer seeking reimbursement or clawback of fees already incurred.

Failure to co-operate with investigation 13.3.3.2

How to decide whether to co-operate where failure to do so will affect indemnification

Most indemnification policies or agreements will contain provisions setting out the need for full co-operation between the employee and employer. At various stages of an investigation, the employee should consider carefully whether it continues to be in his or her best interests to fully co-operate with the employer. As the investigation develops, matters may come to light that indicate the employee's interests conflict, or are likely to conflict, with the employer's. In such circumstances, ILAs should discuss with the employee whether co-operation remains in the employee's best interests and the consequences that will flow from adopting a stance that is at odds with the employer.

© Law Business Research 2021

13.3.4 Ensuring sufficient funds for protracted investigation

13.3.4.1 Cap on insurance policy

D&O policies should be reviewed at the outset and during investigations to ensure the scope and limitations of coverage are understood.

Generally, D&O policies include annual or total aggregate limits, or both. In circumstances where the employer and a number of directors are under investigation or where investigations are becoming protracted, it is not uncommon for the aggregate limit to quickly become exhausted. ILAs should ensure that the scope of any insurance cover is kept under constant review.

13.3.4.2 Commitment of company to continue indemnification

As previously noted, employers will continually assess whether it is appropriate to continue to indemnify employees under investigation. If it becomes clear that the employee has acted outside the scope of employment, the employer is unlikely to continue to provide support unless it would be in its interests to do so because, for example, there is a potential for related civil claims to be made against the employer.

13.4 Privilege concerns for employees and other individuals

13.4.1 In communications with other employees

13.4.1.1 Colleagues or people involved in underlying events

See Chapter 36 on privilege

As a matter of English law, communications between an ILA and third parties will only be protected by privilege if they relate to an existing, pending or reasonably contemplated litigation (in other words, litigation privilege applies). This is not always going to be the case in the context of an internal, or indeed external, investigation.

As such, unless the former colleague or associate of the individual is also implicated in the allegations such that common interest privilege may arise, ILAs should avoid communicating with third parties. Even in circumstances where common interest privilege can be said to arise, this is a developing area of English law and therefore subject to change. ILAs should act with caution and ensure that the common interest between the parties is clearly recorded at the outset.

13.4.1.2 Company counsel

Communications between the employee and legal counsel instructed by the employer will not be privileged unless common interest privilege exists. Whether it exists will depend on the circumstances; even if it does, it will not necessarily encompass all communications with counsel.

© Law Business Research 2021

Interviews conducted during internal investigations by the employer will not be privileged from the employee's perspective; the privilege, if it exists, lies with the employer.[12]

See Chapter 36 on privilege

Use of employer email to conduct privileged conversations 13.4.2

With internal counsel 13.4.2.1

Employees should be wary of any communications with in-house counsel as such communications are unlikely to be protected by privilege.

See Chapter 36 on privilege

Unless the individual forms part of the client group identified within the employer that has the dominant purpose of obtaining legal advice,[13] or unless litigation privilege applies, communications with the in-house counsel will not be protected by privilege.

With external counsel 13.4.2.2

Communications between an individual and an ILA will of course be protected by legal advice privilege. However, there are circumstances in which that privilege may be lost, particularly if it can be shown that the confidentiality in the communication has been lost as it is accessible by third parties.

On balance, it is inadvisable for an employee to use work email accounts to communicate with an ILA as it is likely (depending on the terms of any relevant IT policy maintained by the employer) to lead to a dispute that confidentiality in those communications has been lost.[14]

12 The case of *R (on the Application of AL) v. SFO* [2018] EWHC 856 (Admin) highlights the fact that the SFO is likely to be under increasing pressure to seek waiver of privilege over interview notes for disclosure in subsequent criminal prosecutions.

13 As required following *Three Rivers District Council v. Bank of England* [2003] EWCA Civ 474. This case has been criticised in recent cases: see *Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd* [2018] EWCA Civ 2006 and *R (on the application of Jet2.com Ltd) v. Civil Aviation Authority* [2020] EWCA Civ 35.

14 In *Shepherd v. Fox Williams LLP and others* [2014] EWHC 1224 (QB), it was held that the claimant remained entitled to assert privilege over documents even though they had been accessible to the defendant employer when they were sent to the work email address of an employee of the defendant.

© Law Business Research 2021

14

Employee Rights: The US Perspective

Milton L Williams, Avni P Patel and Jacob Gardener[1]

14.1 Introduction

Unless required to by contract or subpoena, employees and former employees may decline to provide information or documents in connection with a corporate investigation. However, many employers will insist on employee co-operation and may impose disciplinary measures – up to and including termination – on those employees who refuse. In the absence of contractual protections, employees may have no legal right to refuse to submit to an interview, even if their answers tend to incriminate them. A 2016 decision from the United States Court of Appeals for the Second Circuit in *Gilman v. Marsh & McLennan Companies, Inc*[2] is instructive. There, two employees argued that Marsh & McLennan's demand they submit to an interview in an internal investigation constituted state action that infringed their right against self-incrimination. The court rejected this argument, calling it 'the legal equivalent of the "Hail Mary pass" in football'.[3]

Although employees generally cannot refuse to participate in investigations without risking their employment, they do possess various rights implicated

1 Milton L Williams is a partner, Avni P Patel is a senior counsel and Jacob Gardener is a counsel at Walden Macht & Haran LLP.

2 826 F.3d 69 (2d Cir. 2016).

3 826 F.3d at 76 (internal quotation marks omitted). In exceptional circumstances, where the government exerts overwhelming influence over the internal investigation and the employer's decision-making, the employer's actions may be found to constitute state action. See, e.g., *United States v. Stein*, 541 F.3d 130, 136 (2d Cir. 2008) (holding that 'KPMG's adoption and enforcement of a policy under which it conditioned, capped and ultimately ceased advancing legal fees to defendants followed as a direct consequence of the government's overwhelming influence, and that KPMG's conduct therefore amounted to state action').

© Law Business Research 2021

by corporate investigations. The sources of those rights include the employer and federal and state law. With respect to the employer, many companies have policies and procedures for internal investigations. For instance, employee handbooks, company by-laws, written guidelines and employment agreements often contain provisions regarding employee data and document collection, workplace searches, communication monitoring, privacy and confidentiality. These documents may also provide guidance on an employee's right to indemnification for legal fees expended during an investigation or related proceedings. In addition, many companies maintain written policies that protect employees from retaliation for participating in an investigation. These documents, and unwritten, established company procedures, should be considered to understand the protection afforded to employees in an investigation.

Federal and state law also govern the rights of employees involved in investigations. These rights, discussed below, can be divided into four general categories: (1) the right to be free from retaliation; (2) the right to representation; (3) the right to privacy; and (4) the right to indemnification.

The right to be free from retaliation 14.2

Although employees generally have no right to refuse to participate in a corporate investigation, they may be protected from retaliation. A number of federal employment statutes prohibit retaliation against employees who participate in corporate investigations.[4] State and local laws provide similar protection.

Moreover, employees who possess information regarding corporate misconduct have some leverage in that they may become whistleblowers. Whistleblowers are protected from retaliation under federal[5] and state whistleblower laws.

See Chapter 20 on whistleblowers

The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) provides for both civil and criminal penalties for employers who retaliate against whistleblowers. Section 806 of the law governs civil penalties. It prohibits publicly traded companies from retaliating against employees who assist or provide information to law enforcement, Congress, or 'a person with supervisory authority over the employee' regarding activity the employee reasonably believes is a violation of: (1) federal law regarding mail, wire, securities, or bank fraud; (2) an SEC rule or regulation; or (3) any provision of federal law relating to fraud against shareholders.[6]

Section 1107 of Sarbanes-Oxley provides for criminal penalties for retaliation against whistleblowers. Specifically, it criminalises '[w]hoever knowingly,

4 These statutes include Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Labor Standards Act, the Family and Medical Leave Act, the National Labor Relations Act, and the Occupational Safety and Health Act.

5 The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the Consumer Financial Protection Act of 2010.

6 See 18 U.S.C. § 1514A(a).

© Law Business Research 2021

with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense'.[7]

Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) provides anti-retaliation protection for whistleblowers who report possible securities law violations to the Securities and Exchange Commission (SEC).[8] Similarly, Section 748 of Dodd-Frank protects whistleblowers who report violations of the Commodity Exchange Act to the Commodities Futures Trading Commission.[9] And Section 1057, which codifies the Consumer Financial Protection Act of 2010, forbids retaliation against employees who blow the whistle on possible violations of that statute.[10]

Despite their similarities, there are important differences between the whistleblower protections contained in Sarbanes-Oxley and Dodd-Frank. Procedurally, in contrast to Sarbanes-Oxley's requirement that complaints be filed with the Department of Labor within 180 days of the retaliatory act or the complainant's discovery of the retaliation,[11] Dodd-Frank permits an employee to bring a private cause of action directly, without having to go through an administrative agency,[12] and allows the employee to do so within six to ten years, depending on the circumstances.[13] In addition, Dodd-Frank provides more attractive financial incentives for whistleblowers. A whistleblowing employee who prevails under Dodd-Frank may receive up to twice the amount of wages lost due to retaliation, as well as attorneys' fees.[14]

Under Sarbanes-Oxley, by contrast, a whistleblower's recovery is limited to the 'relief necessary to make the employee whole', including reinstatement, back pay, 'special damages' (which includes damages for non-economic harm such as reputational injury, mental anguish and suffering), attorneys' fees and costs.[15]

Critically, however, whereas Sarbanes-Oxley protects employees who report concerns to supervisors at their company, Dodd-Frank does not. Dodd-Frank defines 'whistleblower' to mean a person who provides 'information relating to a violation of the securities laws to the Commission'.[16]

---

7 See 18 U.S.C. § 1513(e).

8 See 15 U.S.C. § 78u-6(h).

9 See 7 U.S.C. § 26.

10 See 12 U.S.C. § 5567.

11 See 18 U.S.C. § 1514A(b).

12 See 15 U.S.C. § 78u-6(h)(1)(B)(i).

13 See 15 U.S.C. § 78u-6(h)(1)(B)(iii)(I)–(II).

14 See 15 U.S.C. § 78u-6(h)(1)(C).

15 See 18 U.S.C. § 1514A(c).

16 See 15 U.S.C. § 78u–6(a)(6). The Supreme Court has held that this provision requires whistleblowers to report to the SEC. See *Digital Realty Tr., Inc. v. Somers*, 138 S. Ct. 767, 776, 778 (2018).

© Law Business Research 2021

The right to representation 14.3

Employees have no automatic right to counsel during an internal investigation,[17] unless contractually provided under the terms of their employment.[18] Nonetheless, employees may choose to retain counsel, particularly if they face liability.

Concerns over individual criminal liability have increased since September 2015, when then Deputy Attorney General Sally Yates issued a memorandum titled 'Individual Accountability for Corporate Wrongdoing'. The 'Yates Memo' stressed the importance of combating corporate misconduct by holding individuals accountable. It listed six steps that should be part of all investigations and prosecutions of corporate misconduct, the first of which is that a corporation's eligibility for co-operation credit depends on it providing the Department of Justice (DOJ) with all relevant facts about the individuals involved in the alleged misconduct. The Yates Memo also stated that all investigations must focus on individuals from the inception of the investigation, and that barring extraordinary circumstances, which must be personally approved in writing by specified DOJ personnel, DOJ attorneys will not agree to any settlement or corporate resolution that dismisses charges or provides immunity for individual officers or employees. The basic principles of the Yates Memo have been incorporated, with various tweaks, in the DOJ's current Justice Manual.

On 28 October 2021, Deputy Attorney General Lisa Monaco announced the DOJ's renewed focus on individual accountability. She declared that the DOJ would restore prior guidance making clear that to be eligible for co-operation credit, companies must provide the DOJ with all non-privileged information about individuals – regardless of position, status, or seniority – involved in or responsible for the misconduct at issue. This announcement ended the approach used by the DOJ since 2018 that allowed companies to limit disclosures to those they assessed to be 'substantially involved' in the misconduct.

Interviews without employee's counsel 14.3.1

An employer may seek to conduct an interview of an employee, either with or without company counsel present, before that employee has appointed counsel.[19] Once the employee offers an account of events, it may be difficult

17 The Sixth Amendment right to counsel is triggered by a custodial interrogation by law enforcement authorities. See *Miranda v. Arizona*, 384 U.S. 436, 478-479 (1966). An internal investigation by a private company does not generally implicate this right.

18 Union employees, however, may insist that a union representative attend any investigatory interview that could lead to the employee's discipline. See *N.L.R.B. v. J. Weingarten, Inc.*, 420 U.S. 251, 256-57, 260 (1975). The union representative may not interfere with the interview. *New Jersey Bell Tel. Co. & Local 827, Int'l Bhd. of Elec. Workers, Afl-Cio*, 308 NLRB 277, 279, 280 (1992). Employers have no obligation to inform employees of their right to union representation or to ask if they would like a union representative present during the interview.

19 If individual counsel is retained, company counsel must be cognisant of Model Rule of Professional Conduct 4.2, which states: 'In representing a client, a lawyer shall not

© Law Business Research 2021

to offer a different one later. When counsel for individuals are appointed, they should obtain all information regarding their clients' prior statements about the subject of the investigation, including requesting any relevant memoranda created in prior interviews. Individual counsel should also request all documents, data and other information pertaining to their clients' involvement in the subject of the investigation. Requests for such information may be directed to the client, company counsel, law enforcement and other witnesses (or their counsel). Even if counsel is not allowed to participate in a client's investigatory interview, they should use the acquired information to prepare their clients.[20]

See Chapters 8 on witness interviews and 16 on representing individuals in interviews

14.3.2 Separate representation arranged by the employer

Whether the employer agrees to arrange for counsel can depend on a number of factors, such as the employee's contractual and indemnification rights, state and local laws, the corporate by-laws, and the potential conflict of interest between the employee and the corporation. Although separate representation of an employee can increase expenses and lengthen the investigation, it can also provide certain advantages to the company. It can reduce any suggestion of improper influence by the company over the employee, which can bolster the company's credibility with the government when reporting the results of the investigation and increase the company's co-operation credit. In some circumstances (particularly when individual counsel has a good working relationship with company counsel), it can facilitate communication with the employee. Company and individual counsel should come from different law firms. Further, arranging for individual representation can deter the government from communicating directly with the employee.

When confronted with multiple employees who warrant separate counsel, employers may seek to reduce costs by arranging for 'pool counsel' to represent the entire group. However, this pool arrangement must be reassessed if a conflict of interest arises within the group.

14.4 The right to privacy

14.4.1 Workplace searches

In most circumstances, an employer can conduct searches of its workplace and computer system to investigate wrongdoing. Such searches are largely unprotected by personal privacy laws as workspaces, computer systems and

communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.'

20 If counsel concludes, after reviewing the available information and conferring with the client, that the evidence establishes the client's guilt, counsel may wish to advise the client to decline an interview to avoid making potentially incriminating statements. Although that may prompt the client's termination, counsel may reasonably determine that termination is inevitable regardless of the client's participation in the interview.

© Law Business Research 2021

company-issued electronic devices are generally considered to be company property. Many companies explicitly address this in written corporate policies and employment agreements. However, unwarranted or unreasonable invasions of privacy during a workplace search may be protected under state law – including state constitutional,[21] statutory[22] and common law.[23]

Employees who use their own personal electronic devices for work should be aware that work-related data stored on those devices belongs to the employer. Therefore, employees are advised to refrain from using their personal devices for work, and instead maintain separate work devices. These concerns arising from the use of personal devices for work have become more salient in the age of covid-19, when many employees are working from home. Therefore, it is all the more important now that employers maintain and update their privacy and bring-your-own-device policies and that these policies be documented, well-defined and require written acknowledgement by employees. If an employer seeks to obtain or review work-related data from an employee's personal device, the employer must be careful to exclude any personal data.

Federal and state law protect employees from unauthorised monitoring of their personal data. The Stored Communications Act (SCA) establishes a civil cause of action against anyone who intentionally accesses without authorisation a facility through which an electronic communication service is provided and thereby obtains access to a wire or electronic communication while it is in electronic storage.[24] Accessing an employee's personal email without permission has been held to violate the SCA.[25] The Computer Fraud and Abuse Act (CFAA) imposes criminal liability on those who gain unauthorised access to a computer, and it permits the recovery of civil damages.[26] In addition, several states have enacted laws requiring employers to notify employees before monitoring their electronic communications.[27] In sum therefore, if an employer

21 See, e.g., Cal. Const. art. I, § 1 (protecting right to privacy).

22 See, e.g., Cal. Lab. Code § 980 (2012) (prohibiting an employer from requiring or requesting an employee to: (1) '[d]isclose a username or password for the purpose of accessing personal social media', (2) '[a]ccess personal social media in the presence of the employer', or (3) '[d]ivulge any personal social media, except' in response to a request 'to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding'; prohibiting an employer from taking adverse action against an employee or applicant for not complying with a prohibited request or demand for access to social media).

23 See, e.g., claims for invasion of privacy, intentional infliction of emotional distress and negligent infliction of emotional distress.

24 See 18 U.S.C. § 2701. The SCA defines an 'electronic communication service' as 'any service which provides to users thereof the ability to send or receive wire or electronic communications.' 18 U.S.C. § 2510(15).

25 See *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 755-59 (N.D. Ohio 2013).

26 See 18 U.S.C. § 1030.

27 See, e.g., Del. Code Ann., tit. 19, § 705; Conn. Gen. Stat. § 31-48d.

© Law Business Research 2021

insists on monitoring its employees' personal devices used for work, clear policies and written consent are critical.

14.4.2 Workplace surveillance

An employer seeking to investigate wrongdoing through electronic surveillance must be mindful of federal and state law.

Title III of the federal Omnibus Crime Control and Safe Streets Act of 1968[28] criminalises the intentional interception of any wire, oral or electronic communication unless at least one of the parties to the communication has consented to such interception or the employer is monitoring or recording employee telephone calls 'in the ordinary course of its business'.[29]

Most states (and the District of Columbia) similarly prohibit electronic surveillance of communications unless at least one party to the communication provides consent. Some, but not all, of these jurisdictions provide exemptions for employer monitoring of employee communications. Eleven states – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania and Washington – prohibit to some degree, either criminally or civilly, surveillance without the consent of all the parties to the communication.[30]

Notably, with respect to email, because employees generally do not possess an expectation of privacy in their work accounts, employers may access personal emails exchanged over these accounts. Employees should be aware that some employers may choose to install surveillance monitoring systems into work accounts, databases and company-provided devices. As technology and communications systems advance, employees should also be conscious of their activities on communications platforms. Some messenger services used by companies, such as Slack, have announced privacy policies that allow employers to download all data from their workspace, including all employee data and messages.

14.5 Covid-19

The covid-19 pandemic has impacted virtually every aspect of society, especially the workplace; the virus has presented a variety of new challenges for employers and employees. Most notably, companies have had to adjust to remote working and social distancing, which, among other consequences, has made it challenging to conduct internal investigations, especially those involving extensive travel and interviews. This may create a temptation to delay investigations until

28 See 18 U.S.C. § 2510 et seq.

29 See 18 U.S.C. § 2510(5)(a).

30 See Cal. Penal Code § 632; Conn. Gen. Stat. Ann. § 52-570d; Fla. Stat. Ann. §§ 934.01 to .03; 720 Ill. Comp. Stat. ANN. § 5/14-1, -2; Md. Code Ann. Cts. & Jud. Proc. § 10-402; Mass. Gen. Laws Ch. 272, § 99; Mont. Code Ann. § 45-8-213; Nev. Rev. Stat. § 200.620; N.H. Rev Stat. Ann. §§ 570-A:2; 18 Pa. Cons. Stat. §§ 5702, 5704; Wash. Rev. Code §§ 9.73.030 to 9.73.230.

© Law Business Research 2021

business life returns to normal. However, delaying investigations carries significant risks, such as failing to prevent further employee misconduct, impairing access to time-sensitive evidence and key witnesses, increasing the possibility that allegations will be leaked to the government or the media, and jeopardising potential co-operation credit from the government. If an investigation, in whole or in part, is going to be delayed, investigators should take steps to preserve potentially relevant information, institute appropriate interim compliance procedures and regularly monitor the matter for urgent developments. If investigators proceed with an investigation using remote interviews, they should take steps to prevent witnesses making unilateral recordings or interviewing in the presence of third parties, and should be mindful that the interviews may be regarded as having occurred in each of the jurisdictions where the participants are located (requiring consideration of each jurisdiction's laws governing privilege and data privacy).

The pandemic has also created new privacy and discrimination concerns. Employers are permitted to take reasonable measures to combat the spread of the virus, including administering covid-19 tests on employees, taking their body temperatures, making disability-related inquiries, and requiring those who are ill to stay home.[31] Although a number of courts have held that employers may require employees to get vaccinated,[32] some states have limited by statute or executive order the ability to require proof of vaccination. If an employer is concerned about an employee's health, it generally may not exclude that employee – or take any other adverse action – solely because the employee has a disability that places him or her at higher risk. Such action is only allowed if the employee's disability poses a 'direct threat' to her health that cannot be eliminated or reduced by reasonable accommodation.[33] Employers may be compelled to grant reasonable accommodations to employees with disabilities that place them at higher risk from covid-19, provided such accommodations do not create an undue burden.[34] Lastly, while the pandemic has forced many

31 See US Equal Employment Opportunity Commission, What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

32 See *McCutcheon v. Enlivant ES, LLC*, 2021 WL 5234787, at *4 (S.D.W. Va. 9 Nov. 2021); *Beckerich v. St. Elizabeth Med. Ctr.*, 2021 WL 4398027, at *9 (E.D. Ky. 24 Sep. 2021); *Bridges v. Houston Methodist Hosp.*, 2021 WL 2399994 (S.D. Tex. 12 Jun. 2021).

33 US Equal Employment Opportunity Commission, What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws..

34 Id. If an employee does not have a qualifying disability justifying a remote working accommodation, the employer may require him or her to come into the office, subject to any contractual exemptions or applicable state and local law (including stay-at-home orders). However, an employee who is infected or quarantined or who is caring for children or infected family members may be entitled to leave from work under the Family and Medical Leave Act, the Families First Coronavirus Response Act, and analogous state law.

© Law Business Research 2021

businesses to downsize, employers may not use that as a pretext for unlawful discrimination. For example, a company cannot use the pandemic as an excuse to lay off its older workers because of their age.

14.6 Indemnification

Among the significant issues that may arise from in-house counsel, and often external counsel, representing the company and not the individual is whether the employee has a right to be indemnified. The right to be indemnified may extend to legal fees, advancement of legal fees and for any potential judgment debt or settlement. As discussed above, an employee has a right to have his or her own counsel, even if the company pushes for joint representation by company counsel, but the complicated question of whether the company must indemnify the employee for costs around separate representation may arise. Determining a company's indemnification obligations requires close review of any agreements and understandings that might give rise to indemnification or advancement of fees. It is critical that an employee communicate closely with company counsel to come to a mutual understanding of the company's obligations.

14.6.1 Determining whether an individual is indemnified

Employees should ask their counsel to assertively engage in communications with the employer and company counsel to determine whether the company will agree to indemnify the individual employee – and if so to what extent – and to advance fees. If the company agrees to, or must, indemnify under any agreement or other source of this right, the employee's counsel should draft and execute a written agreement binding the company. Although the company may seek to impose unfavourable terms, it is generally advisable to reduce the indemnification obligation to writing.

Employees and their counsel should carefully review potential sources of the right to indemnification. These sources may include company by-laws, local law in the state of incorporation, company policies and insurance policies of the employer.

14.6.2 Potential sources of right to indemnification

14.6.2.1 Corporate by-laws

Corporate by-laws often delineate the company's obligation to indemnify an employee's costs arising out of representation for internal investigations or any matters related to his or her official duties. Corporate by-laws require careful review because even if indemnification obligations are provided, they are often listed with limitations or releases from obligation, including limiting obligations to certain employee categories. Limitations and releases include provisions releasing the company from its obligations to repayment of any indemnified cost if the costs subsequently transpire not to be indemnifiable. If these provisions exist, it is likely that the company will require the employee to

© Law Business Research 2021

sign an undertaking letter, in which the employee agrees to repay any amounts advanced if it is later determined that the employee was not entitled to indemnification. Similarly, there is a difference between the duty of an employer to indemnify an employee of costs incurred and any duty to advance defence costs. Corporate by-laws should be reviewed carefully, because absent such language, the employee has no right to advancement of attorneys' fees.[35]

Local law in state of incorporation 14.6.2.2

Several states have state and local laws that impose indemnification obligations on companies for private employees. Review of state and local laws is often overlooked because employees assume indemnification provisions are exclusively contained in corporate by-laws and any employment or subsequent agreements with the company.

For example, under Delaware corporate law, directors generally have a right to indemnification if they are, or face being, parties to a proceeding or subject to investigation, unless they did not act in good faith and in a manner reasonably believed to be in, or not opposed to, the best interests of the corporation.[36] Directors and officers who succeed in their defence are indemnified. On the other end of the permissive spectrum, if a director or officer acts in 'bad faith', they are not entitled to indemnification.[37] Delaware law also allows directors and officers the right to indemnification through advanced costs for pending litigation.[38] In other states, like Oregon and Washington, state law affords directors this same mandatory indemnification if successful on the merits unless the company's articles of incorporation provide otherwise.[39]

California is an example of a state that extends indemnification protections to any private employee, not only directors or officers. Further, the California Labor Code provides that an employee has a right to reimbursement.[40]

Even if state legislation imposes obligations on companies to indemnify legal costs for private employees, however, the employee might not have the right to select his or her own separate counsel. In other words, unless a known conflict exists, a private employee may be forced to use whichever counsel represents the company. New York is an example of a state where the statutes provide that even if a court ordered an employer to indemnify a private employee, the employee would have to show that the specific attorneys' fees in question were 'reasonable' and 'necessary',[41] which places the burden on the employee to show why representation separate from company counsel is

35 In practice, more often than not, by-laws will entitle employees to have their attorneys' fees advanced.

36 See 8 Del. C. § 145(c).

37 *Hermelin v. K-V Pharm. Co.*, 54 A.3d 1093, 1094 (Del. Ch. 2012).

38 See 8 Del. C. § 145(e).

39 See ORS 60.394 and RCW 23B.08.520.

40 See Cal. Labor Code § 2802(a).

41 See N.Y. Bus. Corp. Law § 724.

© Law Business Research 2021

necessary. This places employees in a difficult position if they have reason to believe that their interests would be better served with separate counsel but would have to forgo having certain legal costs covered by their employer. Employees that believe they will be indemnified pursuant to state law should adequately review the statute to ensure that they understand the parameters – and potential limitations – of indemnification obligations at the onset of an investigation.

14.6.2.3 Company policies

Employees should also look at company policies and employment contracts or subsequent agreements as sources of indemnification rights. Individual employees may have contractual indemnification rights in their employment agreements. Even if the company by-laws do not indicate a right to indemnification, a company must honour any obligations in individual employment agreements such as including within the scope of indemnification certain employee categories not otherwise covered by by-laws or state and local laws. As a strategic point, employers may expand the scope of indemnity to ensure co-operation of employees, which may show the company in a more favourable light to any regulator or investigative body.

14.6.2.4 Insurance policies of employer

Some employers may choose to purchase directors' and officers' (D&O) insurance to supplement or provide an alternative to indemnification. If the employer has D&O insurance, the nature of the allegation and the terms of the specific policy may trigger payment of defence costs.

D&O insurance is increasingly important in corporate culture owing to the increase in shareholder, class action, derivative action and other prosecutorial and regulatory investigations targeting not only companies, but also their directors and officers. Directors and officers of companies should carefully review terms, conditions, provisions and exclusions of any D&O policy.[42]

14.6.3 Advocating for indemnification

Companies are not always eager to indemnify employees for representation or costs incurred during an investigation or defence. However, employees should review possible sources of company obligation and advocate for companies to indemnify them for incurred costs or advancement of fees, including before entering any employment or separation agreement.

The employer or company may become more credible and promote efficiency and effectiveness of an internal investigation by ensuring that employees are adequately represented. If company counsel recognises a conflict of interest and the need for the employee to have separate representation, the corporation

42 See, generally, Matthew L Jacobs, Julie S Greenberg, *Basic Principles of D&O Coverage and Recent Developments*, 741 PLI/Lit 29, *35 (2006).

© Law Business Research 2021

benefits if the employee is co-operative. Therefore, the company may assess the employee's involvement and whether failure to pay individual counsel fees or to advance attorneys' fees will make the employee's co-operation less likely. While in some instances employees may be required to co-operate by subpoena, it is in the best interest of the corporation to work jointly with the employee to prepare its own defence and receive information in advance through a joint defence agreement.

In addition, regulators and prosecutors cannot take into account during an investigation whether a corporation is advancing or reimbursing attorneys' fees or providing counsel. Along the same lines, a prosecutor or regulatory body cannot request that a company refrain from taking such action. In 2008, the Department of Justice published the 'Filip Memo',[43] which laid out the principles of federal prosecution of business organisations. The guidelines, codified in the US Attorney's Manual (now called the Justice Manual), state that: 'In evaluating cooperation, however, prosecutors should not take into account whether a corporation is advancing or reimbursing attorneys' fees or providing counsel to employees, officers, or directors under investigation or indictment.'[44]

Situations where indemnification may cease 14.7

Employees should be aware of the circumstances in which a company's obligations to indemnify may cease. As mentioned, a company's obligations to indemnify an employee may be contingent on, and circumvented by, any undertaking agreement between the parties. Further, a company is generally released from its indemnification obligations for any violation of an undertaking agreement (substantive or procedural) and fraud or bad faith.

In some instances, an employee's failure to co-operate with a company's investigation could absolve the company's obligation to cover individual costs. This can create a difficult decision for an individual employee regarding whether to co-operate where failure to do so will affect indemnification. Even if an employee does not want to co-operate with company counsel – internal or external – and submit to an interview or otherwise co-operate, he or she may still be called to produce testimony or information pursuant to a subpoena.

See Chapter 10 on co-operating with authorities

Privilege concerns for employees 14.8

Privilege considerations become central during investigations. Because of the various permutations of attorney–client relationships with both internal and external counsel, it is important for employees to remember that they only enjoy protections over communications with individual counsel. If an employer

43 Memorandum from Deputy Attorney General Mark Filip to Heads of Department Components and United States Attorneys, Principles of Federal Prosecution of Business Organizations 8 August 2008), available at https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

44 USAM 9-28-730 Obstructing the Investigation.

© Law Business Research 2021

requests an interview with an employee, employee counsel and company counsel, the communications and testimony at the interview are not privileged.

An employee and his or her counsel should note whether the company counsel issued a proper *Upjohn* warning and whether it was documented. If an inadequate *Upjohn* warning was given, an employee's individual counsel may attempt to prevent or limit disclosure of any statements made by the employee in an interview where individual counsel was not present.

The Third Circuit established the *Bevill* standard to determine whether a company employee holds a joint privilege with the employer company over communications with corporate counsel, which has since been adopted by the First, Second, Ninth and Tenth Circuits. The *Bevill* standard holds that 'any privilege that exists as to a corporate officer's role and functions within a corporation belongs to the corporation, not the officer'.[45] The Court in *Bevill* extended the privilege to officers and employees in an individual, personal capacity only when the employee satisfies the following five-factor test. First, they must show that they approached counsel for the purpose of seeking legal advice. Second, they must show that when they approached counsel, they made it clear that they were seeking legal advice in their individual capacity rather than in their representative capacities. Third, they must demonstrate that the counsel saw fit to communicate with them in their individual capacities, knowing that a possible conflict could arise. Fourth, they must prove that their conversations with counsel were confidential. And fifth, they must show that the substance of their conversations with counsel did not concern matters within the company or the general affairs of the company.[46] Notwithstanding the foregoing, an employee would be ill-advised to confide in, or speak candidly with, company counsel given the subjective nature of the standard and make efforts to secure personal individual counsel.

See Chapters 8 on witness interviews and 16 on representing individuals in interviews

Finally, as a practical matter, employees should be aware that communications with other employees or colleagues regarding the investigation are not privileged regardless of whether the colleague is also involved in the investigation or represented by the same counsel. Even if an employee believes he or she is sharing attorney communications with other employees who need to know the attorney's advice and who also have an attorney–client privilege with the same counsel because he or she is involved or implicated in the investigation and also represented by company counsel, it is always prudent to refrain from sharing privileged information. In addition, employees should attempt to communicate with individual counsel on personal and non-company devices to ensure that the privilege is protected.

45 *In re Bevill, Bresler & Schulman Asset Mgmt. Corp.* 805 F.2d 120 (3d Cir. 1986).

46 *US v. Graf*, at 8 (citing *Bevill*, 805 F.2d 120 (3d Cir. 1986)).

© Law Business Research 2021

15

Representing Individuals in Interviews: The UK Perspective

Jessica Parker and Andrew Smith[1]

Introduction 15.1

This chapter considers the representation of individuals in three types of interviews: interviews in corporate internal investigations, interviews of witnesses in law enforcement investigations, and interviews of suspects in law enforcement investigations.[2]

Interviews in corporate internal investigations 15.2

When should employees have their own lawyer? 15.2.1

In many corporate internal investigations, it is common for employees not to receive or be offered legal advice, either before or during their interviews. This is because the employee is not normally treated as a suspect in what is commonly referred to as a 'fact-finding investigation'. Their position is analogous to but distinct from an employee interviewed in disciplinary proceedings, in which an employee suspected of misconduct has no right to legal representation at the interview, but is usually entitled to be accompanied by a fellow employee or trade union representative.

1 Jessica Parker and Andrew Smith are partners at Corker Binning.

2 By 'law enforcement investigations' we mean investigations by UK public bodies such as the National Crime Agency and regional police forces exercising a statutory function of investigating criminal offences. Some of these bodies also act as prosecutors, for example the Serious Fraud Office and the Financial Conduct Authority. In other cases, the Crown Prosecution Service will be responsible for prosecuting. There are other types of interviews in law enforcement investigations that fall outside the scope of this chapter, for example interviews of co-operating witnesses under the Serious Organised Crime and Police Act 2005.

© Law Business Research 2021

However, in some corporate internal investigations, the corporate may recommend a lawyer (often called an independent legal adviser or ILA) who can represent the employee. Alternatively, the employee may prefer to benefit from legal advice, regardless of whether a lawyer has been recommended by the corporate.

Legal representation for an employee may be desirable in two main situations. First, if the employee risks self-incrimination or admitting regulatory breaches, there may be a conflict of interest between the employee and the corporate. In particular, conducting the interview without first offering the employee legal representation may place the corporate's lawyers in breach of their professional ethical duty not to take 'unfair advantage' of a third party.[3]

Secondly, legal representation for an employee may be desirable where the employee's acts and omissions determine the criminal or regulatory liability of the corporate, for example where the employee is the 'controlling mind' of the corporate or an 'associated person' for the purposes of the Bribery Act 2010.[4] In these circumstances, the corporate may consider that legal advice will enable the employee to render a more reliable account in an interview – an outcome that furthers the corporate's interests in helping it more accurately to assess its own exposure to criminal or regulatory liability.

15.2.2 The role of the employee's lawyer prior to the interview

While the lawyer will always owe professional obligations to the client (i.e., the employee), the corporate may require the employee to agree to the lawyer acting on restricted terms. Such terms may define the scope of the lawyer's work and outline circumstances in which the lawyer's fees will not be paid or can be clawed back from the employee (e.g., if the employee becomes a whistleblower or is charged with a criminal offence). There may be other terms dictated by the corporate's insurers. However, nothing in such terms can derogate from the lawyer's professional ethical duty to act in the employee's best interests.[5]

It is not uncommon for a single lawyer (or law firm) to be asked to act for a number of employees all of whom will be interviewed in the internal investigation. Whether this is permissible is purely a question of professional ethics.[6]

While the employee's lawyer must be independent from those conducting the investigation, it is nearly always beneficial for the employee's lawyer to form a constructive relationship with the corporate's lawyers. This relationship should enable the employee's lawyer to understand the allegations being

3 Outcome 11.1 of the Solicitors Regulation Authority (SRA) Code of Conduct. However, whether this outcome is likely to be breached in a corporate internal investigation has not been explored in any case law, and will depend on precisely how the interview is conducted.

4 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153; ss.7 and 8 Bribery Act 2010.

5 Fundamental Principle 4, SRA Code of Conduct.

6 See SRA Code of Conduct, Chapter 3: the solicitor proposing to act for two or more witnesses must be satisfied there is no conflict between them, or no substantial risk of a conflict arising in future, unless specified appropriate safeguards are observed.

© Law Business Research 2021

investigated, the employee's perceived role in relation to the allegations, and whether the corporate has reported the allegations to a law enforcement body. The lawyer should seek comprehensive disclosure prior to the interview of all documents the employee will be asked about and ensure that the employee has sufficient preparation time for the interview.

Clearly the employee's lawyer needs competence in the areas of law relevant to the allegations being investigated (e.g., bribery or the Financial Conduct Authority's (FCA) Senior Managers and Certification Regime). This competence will enable the lawyer to pre-empt the questions that are likely to be asked in the interview, to take meaningful instructions from the employee, to structure those instructions in a logical fashion, and to assess how well the employee would perform in the interview. This may require separate advice on employment law as well as advice from other jurisdictions if the allegations are international in nature or the corporate has self-reported to overseas law enforcement bodies.

The work performed by the employee's lawyer should lead to two fundamental tactical decisions. First, is it in the employee's best interests to attend the interview? Second, if the employee attends the interview, how should the questions be answered to advance his or her best interests?

Advising the employee whether to attend the interview 15.2.3

In most investigations, employees are told that they have a duty to co-operate with the investigation under the terms of their employment contract. Failing to attend the interview will ordinarily lead to the employee being suspended or dismissed. However, this outcome should never be the sole or even the primary factor to consider when advising an employee. Of equal or greater importance is the impact of the interview on any existing or future legal proceedings involving the employee.

The employee's duty to co-operate with the investigation is not akin to a statutory compulsion.[7] Equally, however, employees cannot sensibly attend the interview and then elect not to answer certain questions on the basis that they will incriminate themselves. Electing to answer some questions but not others is overwhelmingly likely to lead to the same result as refusing to attend the interview, namely suspension or summary dismissal.

If by co-operating and answering all questions the employee self-incriminates or admits to regulatory breaches, the interview is unlikely to serve his or her best interests. Not only is the employee likely to be dismissed or suspended given the nature of the admissions (the same outcome that would have occurred had he or she refused to attend the interview), but the corporate will obtain a damaging interview record which could be handed over, and used, in a law enforcement investigation. Although the Court of Appeal judgment

7 It is merely a breach of a private employment contract and carries no statutory penalty.

© Law Business Research 2021

in *Director of the SFO v. ENRC*[8] clarifies the circumstances in which an interview record may be protected by litigation privilege, the corporate may choose to waive privilege as a hallmark of its co-operation. The interviewee must therefore be advised that he or she should only proceed with the interview if prepared to accept the real risk that a law enforcement body will ultimately review a lawyer's note or memorandum of the interview, and potentially make important decisions about his or her status in any future criminal or regulatory investigation based on the answers given in the interview.

Whether the record of an interview in an internal investigation constitutes admissible evidence against the employee in legal proceedings has not been explored in any case law. However, there are analogous cases which suggest that, as long as warnings akin to *Upjohn* warnings are delivered at the commencement of the interview, the interview record would probably be admissible in criminal proceedings.[9]

Given that the interview record could be admissible against the employee, the employee's lawyer needs to balance the risk of dismissal or suspension against the risk of increasing the employee's exposure to personal liability in criminal and regulatory proceedings. If the employee is able to deliver a credible account without self-incrimination or admitting regulatory breaches, it will ordinarily serve his or her interests to attend the interview. Equally, there are circumstances in which employees will be advised to attend the interview even though they will admit criminal or regulatory offences, for example, the employee was junior, the offending is relatively trivial, and the employee wishes to be able to say, in any subsequent legal proceedings, that he or she gave the employer an explanation consistent with what he or she now asserts to the law enforcement body. However, if the employee is likely to admit serious offences in the interview, then attending the interview simply to advance mitigation is unlikely to be advisable.

See Chapter 13 on employee rights

15.2.4 The role of the lawyer in the interview

An employee attending the interview will typically be advised that, to advance his or her best interests, answers should be concise, contain no speculation and provide no extraneous detail beyond that required by the particular question. Ideally, this process occurs organically and the lawyer does not need to intervene during the interview. Nonetheless, the lawyer's presence is important, and interventions may become necessary, so as to ensure that:

- the employee is asked questions that are clear and fair;
- the employee is given an adequate opportunity to answer the questions without interruption, intimidation or improper pressure;
- the interviewers do not misconstrue any answers given by the employee;

8 [2018] EWHC 2006.

9 *R v. Twaites and Brown* (1991) 92 Cr App R 106 CA; *R v. Smith* [1994] 1 WLR 1396; *R v. Welcher* [2007] Crim LR 804 CA.

© Law Business Research 2021

- the employee does not inadvertently waive privilege over advice;
- the employee can take advice on an ongoing basis about issues that arise during the interview or previously undisclosed documents which he or she is asked to comment on;
- an accurate record is kept of the questions and answers; and
- the employee raises all material facts, defences and mitigation identified during the preparatory work conducted with the lawyer.

See Chapter 7 on witness interviews

Interviews of witnesses in law enforcement investigations 15.3

Law enforcement investigations are conducted under distinct statutory regimes, depending on the nature of the conduct under investigation and the agency conducting it.[10] However, in general terms, there are two types of witness interviews: interviews conducted voluntarily and interviews conducted compulsorily.

Voluntary interviews 15.3.1

The majority of interviews are conducted without the witness being subject to legal compulsion. In other words, the witness is interviewed as a volunteer. While being interviewed voluntarily may seem attractive in that it suggests a co-operative attitude toward law enforcement, the record of the voluntary interview (including any admissions made by the witness) could be used in evidence against the witness in subsequent legal proceedings. In criminal proceedings, this risk increases if the witness has received legal advice prior to the interview, because it becomes less likely that a court would use its discretionary power to exclude the interview.[11]

If there is a risk, however remote, that the witness will self-incriminate in the interview, it is unlikely to be in the witness's interests to attend voluntarily. In these circumstances, being compelled to attend the interview is likely to be advantageous.

Compulsory interviews 15.3.2

Where a witness owes a duty of confidentiality to another party concerning the subject of the investigation, or is concerned about the potential use of the interview record against him or her in subsequent proceedings, the witness should ordinarily refuse to attend the interview voluntarily. In some circumstances, the witness can be compelled to attend and answer questions under statutory powers available to all major investigators, including HM Revenue and Customs, the FCA, the Serious Fraud Office (SFO) and the police.[12] Where

10 For example, under the Criminal Justice Act 1987, s.1, the SFO has a mandate to investigate serious or complex fraud; the FCA's statutory objectives are set out in the Financial Services and Markets Act 2000.

11 Police and Criminal Evidence Act 1984, s.78.

12 See, for example, Criminal Justice Act 1987, s.2; Serious Organised Crime and Police Act 2005, s.62; Financial Services and Markets Act 2000, s.165.

© Law Business Research 2021

this compulsory power is used, the witness is protected from civil suit for breach of confidence. Moreover, the answers given cannot be used in evidence in criminal proceedings against the witness – an important protection that is not available in a voluntary interview.

There are two exceptions to this latter protection: first, where criminal proceedings are brought in respect of false or misleading statements made during the course of the interview; second, where the witness, who later becomes a defendant, advances a different version of events in subsequent proceedings.

The role of the lawyer and the reasons for intervening in compulsory interviews are similar to those in the interview of an employee in a corporate internal investigation.

See Section 15.2.4

15.3.3 Right to legal representation in a compulsory interview

There is no absolute right to a lawyer in a compelled interview, although usually a lawyer will be allowed to attend. In the context of compelled interviews with the SFO under section 2 of the Criminal Justice Act 1987, this principle was confirmed in *R (Lord and Others) v. Director of the Serious Fraud Office*.[13] In this case the SFO challenged a witness's choice of lawyer on the basis that he was a senior employee of a corporate suspect represented by the same lawyer in that investigation. The SFO refused to permit the lawyer's attendance at an interview and the witness sought relief by way of judicial review of the SFO's decision. Permission for the judicial review was not granted and the Administrative Court upheld the SFO's decision to exclude the lawyer.

The SFO's response to this case was to withdraw its existing guidance on section 2 interviews and issue further guidance in June 2016, which was updated in 2019.[14] This guidance creates inroads into the right to legal representation that go far beyond the factual scenario examined in *Lord*. A request for representation by a lawyer during an interview will only be granted if, in the case controller's opinion, they are likely to 'assist the purpose of the interview and/or investigation or that they will provide essential assistance to the Interviewee by way of legal advice or pastoral support'.[15] The lawyer's attendance is permitted on the 'understanding that they should advise on legal professional privilege but otherwise they must not do anything to undermine the free flow of information which the interviewee, by law, is required to give'. The lawyer may be required to sign an undertaking confirming that they do not advise a suspect in the investigation. One note taker will be permitted to attend alongside the lawyer.

13 *R (Lord and others) v. Director of the Serious Fraud Office* [2015] EWHC 865 (Admin).

14 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/codes-and-protocols/.

15 https://www.sfo.gov.uk/download/sfo-operational-guidance-presence-interviewees-legal-adviser-section-2-interview-internal-guidance/.

© Law Business Research 2021

Despite these attempts to restrict a lawyer's role during the interview, it is important for a lawyer always to act in the best interests of the witness and in accordance with his or her professional obligations.

The Law Society has issued a practice note that is essential reading for those advising the recipient of a section 2 notice.[16]

Any undertaking requested should be carefully considered. The Law Society practice note advises as follows: 'You should consider whether it is appropriate and necessary to agree the undertakings sought by the SFO on a case-by-case basis. You should carefully consider the implication of agreeing to any undertaking and, if necessary, seek to amend the terms of the undertaking before agreeing it.'[17] By way of example:

- Has sufficient information been provided to enable the lawyer to undertake whether he or she acts for another suspect?
- Do the undertakings on confidentiality relate to documents that are actually confidential (i.e., if the witness has obtained them from another source, this undertaking should be drafted to exclude such items)?
- Are the undertakings relating to the provision and retention of pre-interview disclosure practicable?

In respect of the conduct of the interview, the lawyer must give advice that the SFO may consider conflicts with the 'free flow of truthful information'. For example, the lawyer must also ensure that:

- the interview is conducted within the parameters of the section 2 power;
- the SFO respects the statutory exception to its compulsory power, such as a refusal to answer questions that are properly the subject of legal professional privilege;[18] and
- the witness is able to deal with the interview properly: the lawyer must ensure that answers given by the witness are not misconstrued, that the witness has sufficient time to consider the documents put to him or her, etc.

Confidentiality of the interview 15.3.4

At the conclusion of an interview with a witness (and some interviews with suspects), the investigator will often inform the witness that they consider the interview to be confidential and that the witness should not discuss it with anyone other than their legal adviser. There is no legal force in these statements. In *Lord*, for example, the court confirmed that there is no obvious bar to

16 https://www.lawsociety.org.uk/support-services/advice/practice-notes/representing-clients-at-section-2-cja-interviews/#cp21.

17 Law Society's practice note, para. 2.2.

18 Criminal Justice Act 1987, s.2(9). Legal professional privilege may be claimed over any communication between a client and their lawyer seeking or giving legal advice and over communications between a lawyer and a third party if litigation was in contemplation and the document or communication was created for the dominant purpose of litigation.

© Law Business Research 2021

an interviewee discussing their interview as they wished.[19] Indeed, there may be good reason for a witness (or his or her lawyer) to discuss what was learned in an investigator's interview with others; careful thought should therefore be given to whether this would be in the witness's best interests. The only exception to this is where the investigation is a money laundering investigation, in which case thought should be given to whether the prohibition on tipping off set out in section 333A of the Proceeds of Crime Act 2002 applies.

15.4 Interviews of suspects in law enforcement investigations

15.4.1 The caution

Law enforcement interviews of suspects are conducted in accordance with the protections set out in the Codes of Practice (PACE Codes) issued pursuant to section 66 of the Police and Criminal Evidence Act 1984 (PACE). Among the most important of these protections is the caution administered to a suspect at the start of an interview.

An investigator must caution a person if there are 'reasonable, objective grounds for suspicion, based on known facts or information which are relevant to the likelihood the offence has been committed and the person to be questioned committed it'.[20] The failure to administer a caution may render the interview record inadmissible in subsequent criminal proceedings.

The caution is as follows:

> *You do not have to say anything. But it may harm your defence if you do not mention when questioned something which you later rely on in Court. Anything you do say may be given in evidence.*[21]

The caution confers on the suspect a right to silence. It also reminds the suspect that if he or she chooses to answer questions, the answers will be admissible in evidence against the suspect at any criminal trial. Finally, the caution alerts the suspect to a rule called the adverse inference. This rule means that, if the suspect fails to mention a fact that in the circumstances existing at the time could reasonably have been mentioned at the interview and later relies on that fact in his or her defence, there is a risk that the trial judge directs the jury that they may draw an adverse inference against the suspect.[22] The jury could draw an adverse inference, for example, if they found that the reason that no answer was given was because there was no good or true answer that would stand up to scrutiny, or if they found that any subsequent fact raised in the defence could have been fabricated.

19 *R v. Lord and others*, para. 21.

20 See Note 10A to para. 10.1 of Code C of the PACE Codes.

21 *per* PACE Code C, para. 10.5.

22 Criminal Justice and Public Order Act 1994, s.34(1) and (2).

© Law Business Research 2021

Jurors may not be asked about their deliberations and so the impact of a judicial invitation to draw an adverse inference is not known. Nonetheless, it is believed that jurors do not always draw an inference even when invited to do so.

Deciding on the suspect's approach 15.4.2

The single most important decision taken by a lawyer representing a suspect in an interview under caution is whether to answer questions, exercise the right to silence or read from a prepared statement. This decision is rarely straightforward; care must be taken to protect the suspect from a variety of risks, including the risk of making damaging admissions, the risk of being ambushed by previously undisclosed documents and the risk of an adverse inference being drawn in any future trial.

To advise on this decision, the lawyer should seek pre-interview disclosure from the investigator, namely an explanation of the evidential basis of the allegations against the suspect. There is no legal requirement to provide pre-interview disclosure, although case law suggests that where none is given, disclosure is very limited or what is given is misleading, the court may decline to draw an adverse inference or may even exclude the interview from evidence.[23] In practice, most investigators will provide some pre-interview disclosure in an attempt to prevent these outcomes. If the disclosure is limited, for example if it contains a summary of facts with no contemporaneous documents, the lawyer should ask a series of questions to establish what evidence has been collected in the course of the investigation and seek sight of any document that will be put to the suspect in the interview. A note should be taken of these discussions so that it can be used in any subsequent application for exclusion of evidence or objection to an adverse inference.

If thorough disclosure is provided, a full comment interview may add credibility to a defence advanced at trial or give the investigator reasons to re-evaluate the factual basis of his or her suspicions. However, if disclosure is inadequate, answering questions may simply provide an account that is inconsistent with material already gathered by the investigator (and that may be deployed by the investigator during the interview to discredit the suspect's account). Moreover, answering questions without fully understanding the basis of the allegations may simply extend the scope of the investigation into new, problematic areas.

In complex financial crime cases, reading from a prepared statement may often be preferable to a suspect answering questions or exercising the right to silence. An effective prepared statement will set out the salient points in the suspect's defence in a structured format and guard against the risk of the adverse inference being drawn. However, there is always a risk in relying on these statements if disclosure is inadequate, such that the statement could be undermined at a later stage of the investigation or omit facts that could have

23 *R v. Mason* [1987] 3 All ER 481.

© Law Business Research 2021

reasonably been mentioned in interview. Practices vary as to whether such statements should be read out at the beginning or end of the interview.

Lawyers advising a suspect should ask themselves two questions. First, are there factors that may suggest the suspect is not able to provide a full and clear account of the conduct? Second, are there tactical reasons to adopt a certain approach? Some of the factors that feed into these questions are whether:

- there are no facts on which the suspect will rely in his or her defence;
- pre-interview disclosure is so limited that it is not possible properly to evaluate and advise on the case against the suspect;
- limited disclosure may indicate that the investigator's case is weak and there is a risk that the suspect would make admissions that may strengthen the case or lead to new lines of enquiry;
- the disclosure, however briefly put, reveals the type of case that calls for a defence to be put in evidence at an early stage;
- the case disclosed is not based on admissible evidence;
- the conduct under investigation is historic or complex, such that inadequate time or disclosure has been provided to prepare effectively (this may not necessarily be the investigator's strategic decision but because evidence is still being obtained);
- the lawyer knows or suspects that the investigator plans to provide documents in the course of the interview that have not been shown to the lawyer in advance; and
- the suspect is by reason of illness, cognitive impairment, drink or drugs, fatigue or other mental state not able to provide an accurate account or take advice on board.[24]

15.4.3 The lawyer's role in the interview

The lawyer's role in an interview of a suspect is similar to the roles described above when acting for employees in corporate internal investigations or for witnesses in law enforcement investigations. However, there are additional considerations when acting for a suspect. For example, in some circumstances, he or she should be warned not to accuse others of lying or other reprehensible behaviour, as to do so will automatically risk their own 'bad character' (which includes non-conviction material such as disciplinary matters) being admitted in evidence.[25]

15.5 Representing individuals during the pandemic

Coronavirus has created a multitude of challenges for the criminal justice system, a system that regularly relies on face-to-face contact to function. Some

24 If any of these conditions are apparent, the suspect is likely to be unfit to be interviewed and medical advice should be obtained.

25 Under Criminal Justice Act 2003, s.101(1)(g).

© Law Business Research 2021

agencies now routinely use remote interviews and some continue to interview face-to-face with the addition of protective measures.

On 1 April 2020, emergency interview protocols were issued by the police and bodies representing the interests of defence solicitors;[26] these have been updated subsequently, most recently in October 2021.[27] These protocols were agreed to avoid or mitigate the health risks that an interview under caution in a face-to-face setting posed. As the United Kingdom moves into an indefinite period of increased risk from physical contact, the Home Office has conducted an open consultation in which amendments have been proposed to the PACE Codes of Practice C (the detention, treatment and questioning of a suspect) and E (the audio recording of an interview). The intention is for modifications to last for the duration of the pandemic to protect the health and safety of those participating in interviews under caution. The consultation envisages the virtual attendance of a solicitor in the interview process. It permits a solicitor to advise the client and be present in the interview either via live video link or telephone conference link. There is currently no date for the measures proposed in the consultation to be implemented.

When considering whether to represent a suspect in an interview under caution by video link the key disadvantages to virtual attendance are as follows:

- The quality of communication is impaired. Where a representative can only see the interviewee and interviewer on screen, important non-verbal cues can be missed. There is an increased risk of misunderstandings and a reduced opportunity to build trust and rapport.
- Additional care will be required to ensure confidentiality. For example, is the interviewee in a suitable, private environment where your private discussion cannot be overheard?
- Where the interviewee and the officers will be in the interview room together, the solicitor's physical presence can be reassuring to an interviewee. This factor should not be underestimated in a challenging interview or where the interviewee is vulnerable.

Where representing a witness or an interviewee in an internal investigation, the factors outlined above should also be taken into account when deciding whether to meet the interviewee in person or conduct the preparation and interview by video link. Where an interviewee is at home, it will be necessary to consider the challenges of controlling the environment. For example, is the interviewee able to give the matter complete concentration, or are there domestic distractions?

26 National Police Chiefs' Council, Crown Prosecution Service, The Law Society, Criminal Law Solicitors' Association and London Criminal Courts Solicitors' Association.

27 See https://www.cps.gov.uk/sites/default/files/documents/publications/National-Interview-Protocol-COVID19-Version-4-4-Oct-2021.pdf.

© Law Business Research 2021

16

Representing Individuals in Interviews: The US Perspective

John M Hillebrecht, Lisa Tenorio-Kutzkey and Eric Christofferson[1]

16.1 Introduction

When representing individuals in investigations, determining whether to consent to an interview and any interview itself can be pivotal. The following sets forth some potential pitfalls and suggests certain best practices.

16.2 Kind and scope of representation

Even leaving aside the multifarious sorts of industries and issues that can be relevant to the representation of an individual, there are various kinds of representations, presenting different types of challenges.

16.2.1 Representing current or former employees

Most typically in sophisticated white-collar matters, a company is either conducting an internal investigation into suspected misconduct or responding to a government investigation (regulatory or criminal, or both) of similar misconduct. The former often morphs into the latter, one way or the other. In those contexts, the individual client is usually a current or former employee or board member. Inevitably, the individual's relationship with the company is crucial, and can materially impact counsel's approach to the interview. At the most basic level, the company may or may not have an obligation to advance reasonable legal fees and expenses to the client.[2] Even in the absence of a contractual or other obligation, the company will sometimes agree to do so. In either scenario, the company might impose a cap or other conditions on payments. In any event, there are significant advantages to the client establishing a co-operative

See Chapters 4 on self-reporting to authorities and 20 on whistleblowers

1 John M Hillebrecht, Lisa Tenorio-Kutzkey and Eric Christofferson are partners at DLA Piper.

2 See, e.g., 8 Del. C. § 145 (discussing advancement).

© Law Business Research 2021

and cordial relationship with the company (including, at minimum, access to documents and other information) – although this is not always possible.

Pool counsel 16.2.2

At times, largely for reasons of efficiency and economy, the client may be one of multiple individuals a single lawyer concurrently represent as a 'pool' of clients who are witnesses or potential witnesses in the same investigation – subject to the ethical rules governing conflicts of interest and confidentiality.[3] This usually occurs where the members of the pool are viewed, at that time, as less culpable and whose interests are thought to be aligned. Such an arrangement presents obvious advantages to each individual. Pool counsel, by definition, obtains a broader perspective and usually has access to more documents than he or she would otherwise, has the benefit of each client's recollection, and can use insights gleaned from the first client's interview or interviews to prepare for subsequent client interviews. To be clear, it is usually best practice not to 'cross-pollinate' clients (by, for example, telling one client what another said about a particular issue), but pool counsel can appropriately use such information to formulate questions and strategies. Before agreeing to represent multiple individuals, counsel must take substantial steps to ensure that there are no conflicts, document the risk of future conflicts and the waiver of any future conflicts in appropriate engagement letters, and remain hyper-vigilant for developing conflicts.[4] The authors recently experienced a situation in which it emerged – a year into representing a pool of individuals – that one client had negative information about a second client (information both had concealed), leading to significant issues during fraught negotiations with the government regarding one of the two clients. Only the existence of an appropriate engagement letter forestalled more serious problems.

Joint defence agreements 16.2.3

Although 'entering into a joint defense agreement is often, indeed generally, beneficial to its participants, like skating on thin ice, dangers lurk below the surface'.[5] These dangers are illustrated by court rulings disqualifying counsel based on a joint defence agreement, precluding counsel from cross-examining a defector who becomes a cooperating witness, and holding that communications thought to be protected by a joint defence agreement were not in fact privileged.[6] Most of these risks can be mitigated if counsel for the participants consider, discuss and record in some fashion the parameters of their agreement,

3 See, generally, Association of the Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2019-4: *Representing Multiple Individuals in the Context of a Governmental or Internal Investigation (Opinion 2019-4).*

4 See, generally, Opinion 2019-4.

5 *United States v. LeCroy,* 348 F. Supp. 2d 375, 387 (E.D. Pa. 2004), as amended on reconsideration (10 Jan. 2005).

6 See, generally, *United States v. Hatfield*, 2009 WL 3806300 (E.D.N.Y. 2009).

© Law Business Research 2021

including the consequences of one or more participants withdrawing from the agreement.[7] On more than one occasion when the authors represented individuals, we received a voluminous quantity of documents from the clients' former employers, all Bates-numbered to the effect that they were produced pursuant to a joint defence agreement, when there had been no discussion about any such agreement. The tendency of many practitioners to prefer informal joint defence agreements with no specific clarity or agreement on the consequences of withdrawal is puzzling, and the consequences can be severe.[8]

In some jurisdictions, including the Southern District of New York (SDNY),[9] practitioners often prefer to use verbal joint defence agreements. While the agreement need not be recorded in writing, there are numerous advantages to doing so. Although courts may find the existence of a joint defence agreement, despite the agreement being purely verbal, the existence of a written document obviates this inquiry. In a December 2018 decision, a judge in the SDNY held that a former employee failed to establish a common interest agreement with his former employer – even though the individual's lawyer emailed company counsel a draft document with the subject line 'Common Interest Privilege Document', specifically noting that the draft document was being shared 'pursuant to our common interest', without any objection or clarification from company counsel.[10] This underscores the importance of documenting explicitly the existence of such an agreement.

Companies under investigation will at times enter into a joint defence agreement with employees or, more commonly, former employees. We have seen such agreements stating that information disclosed to the company will not be disclosed to the government or third parties. This practice is problematic where a company would prefer to disclose illegal or wrongful conduct to the government and minimise its exposure by obtaining co-operation credit, or where the company operates in a regulated industry that imposes a legal obligation on the company to disclose wrongdoing. As a result, counsel for a corporation typically include language in the joint defence agreement that explicitly authorises the corporation to disclose joint defence materials (or a subset of them) at its sole discretion. This kind of joint defence agreement is little more than a glorified *Upjohn* warning.[11] In representing entities, the authors have in the past used joint defence agreements that protect most joint

See Chapter 4 on self-reporting to authorities

7 Unfortunately, far too often the sum total of counsels' 'discussion' along these lines can be summarised as 'This is a joint defence meeting, right?'.

8 See John M Hillebrecht and Jessica Masella, 'Understanding Joint Defense Agreements: The Implications for White-Collar Defendants in the Second Circuit,' *New York L. J.* (25 Jan. 2019).

9 The Southern District of New York (SDNY), centred on New York City, is home to many of the US Department of Justice's (DOJ) most significant international prosecutions and one of its largest US Attorneys' Offices.

10 *SEC v. Rashid*, 17-cv-8223 (PKC) (S.D.N.Y. 13 Dec. 2018).

11 See, generally, *Upjohn Co. v. United States*, 449 U.S. 383 (1981). See also Chapter 8 on witness interviews.

© Law Business Research 2021

defence materials – strategy discussions, draft work product, updates on interactions with the government – but specifically carve out 'historical' interviews of the individual, which are governed by a standard *Upjohn* warning. As a practical matter, however, whatever the form of the joint defence agreement, an individual may have little choice but to agree so as to obtain information (including documents) necessary to present a defence.

Whether to be interviewed 16.3

Internal investigation 16.3.1

At times a client faces real risk in consenting to an interview by the company. Admitting misconduct, even mere violations of company policy well short of criminal violations, can result in discipline, termination and severe financial consequences. Also, one must assume (and advise one's client to assume) that the company will disclose its version of the interview to the government. Hence, before consenting to an interview, it is crucial to understand the facts (including the documents, the context of the transaction or trading strategy, etc., and the client's version of events), as well as the views of company counsel (to the extent they can be elicited). That said, the client often faces a Hobson's choice. The company's advancement of fees (which the client may regard as crucial) may well be conditioned on co-operation and, more fundamentally, in the United States (as opposed to virtually all EU Member States) an employer can generally fire an executive who refuses to be interviewed.[12] Even where there is some degree of risk, when the client wants to continue employment, protect his or her financial situation, or simply continue working for a different employer in the same regulated industry, the incentives to consent to an interview will be strong. Even leaving those concerns aside, failure to consent to an interview will almost certainly lead to an end to reciprocal co-operation from the company – halting the flow of documents and updates and putting an end to coordination. Obviously, there will be cases where the risks of a truthful interview are so palpable that, regardless of the consequences, declining to be interviewed is the only prudent choice. Similarly, many individual clients face close to no risk. The troublesome choices concern those clients who fall in between.

Government investigation 16.3.2

Consenting to a government interview obviously carries additional risks. Therefore, assessing the client's exposure in advance is even more crucial in this context. In addition to assessing the facts and documents, prudent counsel will seek the views of company counsel, speak to counsel for other potential witnesses

12 See *Gilman v. Marsh & McLennan*, 826 F.3d 69 (2d Cir. 2016); see also Michael D Hynes, Brett Ingerman, John M Hillebrecht, 'Second Circuit Affirms Employers' Right to Terminate Employees Who Fail to Cooperate With Internal Investigations,' *DLA Piper Client Alert* (1 Jul. 2016), https://www.dlapiper.com/en/us/insights/publications/2016/06/second-circuit-affirms-employers/.

© Law Business Research 2021

(whom company counsel will usually identify), and if applicable review public record documents, related civil lawsuit filings and media reports (and, increasingly, blogs and other internet commentaries). Equally important are the views, if they can be obtained, of the government lawyers seeking the interview. The United States Department of Justice (DOJ) has a formal taxonomy identifying whether an individual is viewed as a 'target', 'subject' or (less formally) witness.[13] Often, but not always, counsel representing an individual can at minimum get an Assistant US Attorney to answer a question regarding the client's formal status (although it is imperative that the client understand that the status can always shift). Other agencies – for example the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) – usually will not provide even such minimal information, but there are frequently exceptions. Of course, in the United States, an individual's right to remain silent and decline to be interviewed is protected by the Constitution. Many of the same considerations that influence the decision whether to be interviewed by company counsel can also apply here. There may be times when the right strategic decision is to proceed with a voluntary interview (under the limited protection of a proffer agreement, as discussed below), to provide context or explanation. In other cases, the risks may clearly outweigh any potential rewards. In some relatively rare circumstances, reluctance to agree to an interview may be used as a point of leverage in negotiating a non-prosecution agreement or an immunity order (although even in those cases, prosecutors will universally insist on an interview before finalising any such resolution).

Of course, even when contemplating a government interview there are often similar employment-related considerations – an obligation to co-operate to avoid a cut-off of legal fees, termination of employment, or even attempted clawbacks of vested bonuses, etc. And, again, certain executives in regulated industries (e.g., registered broker-dealers) can be easily placed between a rock and a hard place. Also, unlike company counsel, the government can always threaten to use grand jury or other subpoenas.[14]

See Chapter 14 on employee rights

16.4 Preparation for interview

For both internal and government interviews, the typical preparation is much the same. This is where having a good relationship with company counsel becomes so important. If company counsel has provided the key documents, identified counsel for other individuals and shared (within reason) the focus of the investigation (from the company's perspective or that of the government),

13 See, generally, Justice Manual § 9-11.151.

14 The foregoing discussion focuses on the US perspective for individuals located in the United States. For clients located abroad, the calculus may differ in nuanced ways. Among other things, the ability of companies to compel co-operation is markedly less in other jurisdictions (e.g., the European Union) and the ability of US agencies to effectively subpoena persons abroad (through mutual legal assistance treaties or otherwise) is much more limited. (See Chapters 11 on production of information to authorities and 28 on extraterritoriality.)

© Law Business Research 2021

counsel for the individual client will be well positioned to prepare the client for the interview. Conversely, if company counsel has not been co-operative, preparing the client becomes more difficult. Counsel should in any event push the interviewer (company counsel or the government) to identify in advance the topics to be covered and to share in advance the documents to be used during the interview. How much of this is actually made available varies enormously, based on a number of factors. Sometimes everything requested is supplied; sometimes minimal information is forthcoming; but usually the requests are partially satisfied. As a very general observation, certain government entities (e.g., the CFTC) are usually more forthcoming than others (e.g., the DOJ). In any event, there is no harm in asking, if necessary repeatedly.

Even where company counsel shares 'all' the key documents, more often than not crucial – unfortunately, at times the most crucial – documents are omitted. Often, company counsel will produce to the individual client's counsel 'all' the documents the client saw in real time that have been produced to the government and a separate subset of the most important documents. One should never rely on the company's selection. Instead, counsel should run targeted searches on the broader universe of documents. Even then, counsel must bear in mind that that universe (1) obviously does not include documents produced by other entities (which are frequently encountered for the first time when the client is confronted with them during a government interview or SEC testimony), (2) might not include all documents produced by the company and (3) might also not include other documents (texts, instant messages, WhatsApp messages, private emails, etc.) that may have escaped the company's net. In this regard, it is important to remember to ask the individual client early on whether he or she has access to any pertinent documents or communications (including texts and other messages on a work or personal cell phone or other device).

Recognising these limitations and risks, the documents are typically an essential part of preparing for an interview. It is often helpful to conduct a preliminary debriefing of the client without delving too deeply into large numbers of documents. Then, armed with the context and insights provided by that preliminary conversation, counsel typically spends substantial time alone with the documents – reviewing, highlighting, annotating, cross-referencing and generally striving to internalise the pertinent documents. While junior lawyers will typically perform the initial cut of such a review on whatever electronic document review platform they favour, depending on volume and lawyer predilections, it is often easier for the senior lawyer to review and annotate the most significant documents in hard copy, in binders, with highlighters and post-it flags. Every lawyer's methodology will differ, but the point of the exercise should be a constant: identify those documents that are central to the narrative; flag the phrases, paragraphs and emoticons that will grab the attention of a prosecutor, regulator or company counsel; and put together a comprehensible chronology.

A written chronology is often a helpful vehicle to identify salient points and, at a minimum, provides a helpful tool to refresh recollections. During the life of many investigations, there will often be dormant periods where months

© Law Business Research 2021

go by without much or any activity. When the SEC subsequently calls, having a detailed chronology document to reference is a good way to get back up to speed quickly. In building out a chronology, the precise time of day a message was sent is often overlooked. At times, such details support inferences, good or bad, and the reviewing attorneys must be sensitive to that.

Once counsel has done their level best to carefully scrutinise and organise all the relevant documents available, they should be reviewed in detail with the client. In some cases, there are multiple discrete issues (e.g., a revenue-recognition matter raising different issues for a company's different customers) and somewhere there is really a single issue (e.g., an insider trading investigation focused on a single trade by one trading desk). In the former situation, one would generally break up the documents by issue, whereas, in the latter, chronological order usually makes most sense. Even in a case involving multiple different issues, it is important not to be rigidly siloed. Often, the fact that an email or text regarding one subject was sent shortly before a seemingly-unrelated message regarding another can loom large as to the client's state of mind or other important issues.[15]

After reviewing and organising the documents, the client should be walked through them. It often makes sense to provide the client with a collection of the pertinent documents in advance. (On occasion, company counsel will put restrictions on the use of the documents it has provided, including precluding the individual client from reviewing the documents outside the presence of counsel. Where required, clients can review the documents with a junior lawyer or paralegal in the room.)

An important goal of such preparation is to refresh the client's recollection as to documents and events that often are from years earlier. However, almost invariably, portions of some documents will suggest improper conduct as to which the client must be prepared (if possible) to offer a cogent explanation. Sometimes what looks bad to an outside observer turns out to be perfectly proper when put in the context of the industry or transaction at issue. Sometimes what looks bad is truly a joke or sarcasm. In addition, sometimes what looks bad is, frankly, bad.

In identifying potentially problematic aspects of documents, it is important for counsel to put his or her prosecutor's cap on and cast a jaundiced eye on the documents. To the extent possible, it is also important to speak with counsel for other individuals who received the same document to try to elicit the other individuals' understanding of it and the views of the government or company counsel (to the extent there have already been interviews).

One strategic issue that sometimes arises has to do with whether ignorance is bliss. There may be times when *not* refreshing the client's recollection or, more frequently, not educating him or her about an issue (e.g., an accounting rule, a regulatory requirement) makes sense.

15 Some of the authors have had the unpleasant experience of realising such a connection only in the middle of a DOJ interview, a situation that should be avoided at all costs.

© Law Business Research 2021

Once the client is as well versed in the documents and other information at issue as can be expected, it is sometimes a good idea to pressure-test his or her explanations and recollection by conducting what is tantamount to a mock cross-examination. This enables the client to become familiar with limiting answers to what he or she knows and remembers, to avoid speculation or characterisations, and to make what was known and understood at the time as opposed to now (following focused review of documents and awareness of the investigation).

Procedures for government interview 16.5

After tentatively deciding to consent to a government interview, it may be prudent to preface the actual client interview with an attorney proffer. These are more commonly used with some government agencies than others. For example, the Antitrust Division of the DOJ commonly welcomes them. Although practices differ among jurisdictions and government regulators, typically counsel would prepare a detailed outline of a proffer, vetted and approved by the client, and stick to it while presenting to the government.

Counsel should inform the government that the proffer is hypothetical but that the information is what counsel expects the client would say. Counsel should then recount the information prepared in advance and typically not answer any questions the government asks with additional information not vetted with the client. The purpose of such a proffer is to gauge the government's view of the client's exposure. Typically, an attorney proffer is used in the context of DOJ criminal investigations where counsel believes the client is in some degree of jeopardy. Often the proffer will conclude with some version of: 'If the client tells you what counsel has just summarised, would you agree that a non-prosecution agreement would be proper?'[16]

Some years ago, such proffers were very common in criminal cases, particularly where counsel was seeking a co-operation agreement or non-prosecution agreement. Many US Attorney's Offices have in recent years taken the position that an attorney proffer is no different from a client proffer in that the attorney's statements are treated as statements of the client for purposes of the Jencks Act and therefore must be disclosed to defence counsel if the client becomes a government witness.[17] Accordingly, prosecutors have been more reticent about agreeing to attorney proffers.

Assuming the decision is made (either given positive feedback from an attorney proffer or otherwise) to go forward with the government interview or proffer, a number of important preliminary matters must be resolved in

16 Some jurisdictions (such as SDNY) often use non-prosecution agreements for individuals, while others (such as the District of Massachusetts) never do.

17 18 U.S.C. § (Jencks Act); see, generally, *United States v. Triumph Capital Group*, 544 F.3d 149, 161 to 165 (2d Cir. 2008) (reversing conviction because government failed to produce government notes of an attorney proffer).

© Law Business Research 2021

advance. Perhaps most importantly, counsel must clearly explain to the client – and document – all the risks and benefits of making a proffer, and that it would be voluntary and the Fifth Amendment generally precludes anything but a voluntary proffer.[18] Equally fundamentally, counsel must confirm which agencies, and what offices from each agency, will be attending; not only may the risk profiles differ, but each agency may have different ground rules, including different proffer agreements or no proffer agreements at all.

Although, as discussed below, many proffer agreements today provide imperfect protections, they do provide some protection. Accordingly, one crucial requirement of any proffer agreement is a 'most-favoured nation' clause – a commitment from the government agency that it will not share the substance of any proffer with any other agency (foreign or domestic) not bound by the agreement. In this regard, the standard proffer agreement used by the SEC and the typical proffer agreement used by many US Attorney's offices provides that they will not share the proffer with another enforcement agency unless that agency agrees to be bound by the terms of the proffer agreement.

The most common types of proffer agreements (such as those used by the SEC and most US Attorney's offices, including the SDNY) have become longer and more complicated over the years. But the basic minimal protection provided by such an agreement has long ensured that the government cannot use the words the client says in the proffer as direct evidence in seeking an indictment (or filing a civil complaint) or as proof in the government's case-in-chief. This is a material benefit to the client. Absent the proffer agreement (or the agreement by the government to take a proffer subject to the plea-negotiation protections of Federal Rule of Criminal Procedure 11 or Evidence Rule 410 – which the authors have never known to have happened), the government could simply treat the client's statements as a confession and use them accordingly.

However, the exceptions that have been added to these typical proffer agreements over the years, largely supported by the courts, have denuded this basic protection of much of its robustness. Indeed, many savvy practitioners as a matter of near uniform policy will virtually never advise their clients to proffer. One thing is patently clear: if the strategy of consenting to a proffer does not succeed and the client ends up getting indicted, the fact that the client proffered will almost invariably put the client in a worse position.

Assuming the client told a version of his or her state of mind or other issues inconsistent with the government's view of those matters, the typical proffer agreement permits the government to prosecute the client for false statements – basically, for denying culpability or contradicting what others say.[19]

---

18 Curiously, if a proffer does not produce the desired result, some clients have a tendency to forget that the risks were clearly explained to them.

19 See, e.g., *United States v. Percoco*, 16 Cr. 776 (VEC) (S.D.N.Y. 11 December 2017) (individuals who proffered exculpatory explanations during meeting with government after being

© Law Business Research 2021

More commonly, the government uses various terms of the typical proffer agreement to essentially eviscerate the ability a defendant who has proffered to defend himself or herself. Years ago, the typical agreement allowed the government to impeach a defendant who takes the stand with arguably inconsistent statements from the proffer session. That baseline exception has been expanded throughout the years. It is now broadly accepted that if defence counsel makes an argument in opening statement arguably contrary to the proffer statements or cross-examines government witnesses in the wrong way, the government can use the proffer statements – an obviously devastating piece of evidence.[20] Even something as simple as offering documentary evidence tending to show that the defendant was not at the scene of the crime can have the same effect.[21] In at least one case, *omissions* from a proffer statement were deemed admissible based on cross-examination of a government witness.[22]

Therefore, the risks of a proffer, and the loopholes in standard proffer agreements, are very substantial. Again, counsel must make a risk assessment, weigh the pros and cons, and explain everything clearly to the client and document it. Some practitioners do not insist on a proffer agreement in all instances, preferring to send the signal that the client has nothing to hide. It is the rare case where one should be comfortable with that approach. Most prosecutors view a proffer agreement as standard and few, if any, draw invidious conclusions from a lawyer asking for one for his or her client. Indeed, in the authors' experience one need not even ask, because most prosecutors view it as part of their regular practice.

Probably the last significant preliminary matter (other than pressing, yet again, for advance notice of the documents and topics the government expects to cover) is to determine in what fashion the government agency intends to record the interview. At least some government agencies (in our experience, often Inspectors General of various executive branch agencies) have a policy of seeking to audio-record voluntary interviews. Counsel and client should only consider consenting if the agency agrees to share the recording.

In the ordinary course (and certainly in the typical DOJ and SEC interviews), the government will have a designated note-taker (generally a law enforcement agent in a DOJ investigation) using a laptop or pen and paper. It is crucial that counsel for the client has a note-taker who has clear instructions

---

'told that they were "subjects" of the investigation', not 'targets', subsequently indicted for false statements.)

20 See, generally, *United States v. Barrow*, 400 F.3d 109, 113 to 119 (2d Cir. 2005) (where proffer agreement stated that statements could be used 'as substantial evidence to rebut any evidence offered or elicited, or factual assertions made by' defence, assertion in opening that another person made certain specific narcotics sales opened the door to prosecution using proffer statements in case-in-chief which discussed drug dealing more broadly; 'proper rebuttal is not limited to direct contradiction').

21 See, generally, *United States v. Roberts*, 660 F.3d 149 (2d Cir. 2011).

22 *United States v. Vella*, 2011 WL 652752 (3d Cir. 2011).

© Law Business Research 2021

as to what he or she should be doing. Unlike notes of a preparation session protected by attorney–client privilege, notes of a proffer to the government are protected only as work product. The note-taker in that context should strive to record all substance, even at times in 'Q and A' fashion and including interjections, objections, and clarifications by counsel for the client. While in the authors' experience it happens rarely, there are times when the government's notes as to a proffer are completely wrong on crucial issues (e.g., state of mind 'at the time' of the conduct in question) and the existence of painstakingly detailed notes proved to be an essential weapon in arguments with the DOJ and the SEC. Accurate, detailed note-taking is a must.

See Chapter 37 on privilege

Every proffer interview is different. Government lawyers are only human, so the approaches and temperaments of those lawyers run the gamut. Some ask almost entirely respectful open-ended questions. Some start an aggressive cross-examination shortly after initial introductions. Some are respectful and even-keeled but relentlessly ask the same exact question over and over again in an effort to get the client to shift his or her answer and adopt a specific formulation or term that is important to the prosecutor's theory. These all happen – often during the same interview – because in a typical sophisticated white-collar matter, there can be two, three, four or more government lawyers asking questions. When this is the case, the individual client's lawyer must not be 'a potted plant'. The practitioner has a duty to stop a client answering unfair questions, to rephrase questions that are formulated in a misleading fashion, and to challenge the government lawyers when they misstate the client's earlier answers or misleadingly summarise documents or ask questions about one document while ignoring another equally relevant one (which counsel will hopefully know because he or she is conversant with all the documents that have been produced). A good proffer is one where counsel largely stands mute. But one cannot be shy when shenanigans like those summarised above are playing out. To be clear: the government lawyers will not like it. They will accuse you of 'coaching' the client. They may ask you to step out of the conference room and tell you (in essence) to shut up. That is them doing their job. But you have to keep doing your job – respectfully, strategically and within reason. Counsel will, of course, have prepared the client for this potential dynamic.

16.6 Conclusion

Representing individuals in white-collar matters is always fraught with risk. The interview – whether by company counsel or the government – is a key step in any investigation, and one that typically crystallises the risks to the client. Advising a client on whether or not to consent to such an interview is thus something that must reflect your considered judgement. A well-prepared client, whose context you fully understand and whose documents you are confident have been reviewed, may materially advance his or her position by consenting to such an interview. But these risks should always be in the forefront of your mind.

© Law Business Research 2021

17

Individuals in Cross-Border Investigations or Proceedings: The UK Perspective

Richard Sallybanks, Anoushka Warlow and Alex Swan[1]

Introduction 17.1

In any cross-border investigation, invariably suspects will be located in different jurisdictions, subject to investigations by authorities from different jurisdictions, or both.

This chapter looks at the key issues that can arise when acting for an individual present in the United Kingdom and subject to criminal investigation or proceedings here and in one or more overseas jurisdictions.[2]

Cross-border co-operation 17.2

See Chapter 9 on co-operating with authorities

The United Kingdom might co-operate with overseas agencies or regulators in various ways when investigating or prosecuting an individual, ranging from informal 'intelligence sharing' to mutual legal assistance (MLA). The main domestic legislation governing MLA in the United Kingdom is the Crime (International Co-operation) Act 2003 (CICA), Part 1 of which deals with criminal cases.

The United Kingdom is party to a number of bilateral and multilateral MLA treaties. While it is not necessary for an MLA treaty to exist between the relevant countries for a request to be made under CICA, requests are more likely to be successful where a treaty basis exists. Before the United Kingdom's exit

1 Richard Sallybanks is a partner, and Anoushka Warlow and Alex Swan are senior associates at BCL Solicitors LLP. The authors would like to thank Greta Barkle (associate) and Evgeni Voznoi (legal assistant) for their assistance in updating this chapter.

2 Whereas England and Wales have a common legal system, there are certain substantive and procedural differences in the Scottish and Northern Irish systems. This chapter focuses on the English and Welsh legal system.

© Law Business Research 2021

from the European Union, there was concern over how co-operation with EU Member States would be governed following Brexit. On 24 December 2020, the United Kingdom and the European Union signed the UK-EU Trade and Co-operation Agreement (TCA), which includes specific provisions on co-operation and MLA, and facilitates the application between EU Member States and the United Kingdom of certain previous MLA treaties and conventions.[3] While the TCA ensures there remains a strong co-operative relationship, certain investigative tools, such as European investigation orders,[4] can no longer be used.[5]

MLA requests are usually made to the UK Central Authority (UKCA)[6] through a formal international letter of request. The UK Home Office has published detailed guidance on how foreign authorities can make such requests.[7] MLA requests will only be considered appropriate, however, when the request is for evidence (and not intelligence).[8]

A formal MLA request is not required where overseas police and other law enforcement agencies request assistance directly from their UK counterparts. A number of UK agencies[9] can receive direct requests, and often this form of co-operation (also known as mutual administrative assistance) is governed by data sharing agreements or memoranda of understanding.

---

3 In particular, the 1959 European Convention on Mutual Assistance in Criminal Matters, the 1978 Additional Protocol to the European Mutual Assistance Convention and the 2001 Second Additional Protocol to the European Mutual Assistance Convention.

4 A European investigation order is made by a judicial authority in one EU Member State to have specific investigative measures carried out in another. Its purpose is to facilitate and speed up assistance in criminal investigations provided between Member States.

5 In addition, the United Kingdom no longer has access to the Schengen Information System or the European Criminal Records Information System.

6 The UKCA is the Home Office department responsible for receiving, acceding to and ensuring the execution of MLA requests in England, Wales and Northern Ireland. Her Majesty's Revenue and Customs (HMRC) is responsible for MLA requests in England, Wales and Northern Ireland relating to tax and fiscal customs matters. The Crown Office is responsible for MLA requests in Scotland, including devolved Scottish matters.

7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf. Following Brexit, the provisions of the EU Framework Decisions 2003/577/JHA (on Mutual Recognition of Freezing Orders) and 2006/783/JHA (on Mutual Recognition of Confiscation Orders) and the replacement Regulation 2018/1805 no longer apply to the UK. As such, requests for assistance from or to EU Member States in relation to restraint and confiscation should be made under the provisions of Title XI of Part 3 of the UK–EU Trade and Cooperation Agreement.

8 Crime (International Co-operation) Act 2003, s.7(2).

9 These are: the UK Liaison Bureau at Europol via the National Crime Agency (although the United Kingdom is no longer a member of Europol following Brexit, the UK's ongoing co-operation with Europol is provided for within Title V of Part 3 of the UK–EU Trade and Cooperation Agreement); Interpol via the National Crime Agency; UK Visas and Immigration; HMRC; Police Services; Financial Intelligence Units; Asset Recovery Offices.

© Law Business Research 2021

In some instances, cross-border co-operation may extend to the establishment of a joint investigation team (JIT) between investigating agencies in more than one country.[10] Creating a JIT is another way information or evidence can be shared without the need for MLA.

Practical issues 17.3

Asset freezing and restraint 17.3.1

During a cross-border investigation, an overseas authority may use law enforcement co-operation to identify and trace an individual's assets in the United Kingdom[11] and seek to freeze or restrain those assets. The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 (the 2005 Order) sets out the provisions for the United Kingdom to respond to and co-operate with other countries in freezing and confiscating assets.[12] Under section 444(1)(a) of the Proceeds of Crime Act 2002 (POCA), property in the United Kingdom can be frozen in accordance with an external request relating to proceedings for the recovery of criminal proceeds.[13]

In the first instance, external requests will be addressed to the Secretary of State for the Home Department (SSHD) who will in turn refer the matter to the relevant UK authority.[14] The relevant authority will then apply to the Crown Court for the assets to be restrained. For the Court to give effect to an external request the property in England and Wales must be identified, a criminal investigation or proceedings relating to the relevant offence must have commenced in the requesting state and there must be reasonable cause to believe that the alleged offender has benefited from their criminal conduct.[15] Furthermore, under section 447(8) of POCA, the criminal conduct must meet the dual criminality requirement, in that it must also amount to an offence in the United Kingdom, or would do so if it occurred here.

10 Police Act 1996, s.88, (as amended by sections 103 and 104 of the Police Reform Act 2002), and the International Joint Investigation Teams (International Agreements) (EU Exit) Order 2019/274.

11 Any information concerning asset tracing should be sought through police co-operation and financial intelligence units before an MLA request is made. The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005, at Articles 202 to 207, governs how property or sums of money specified in external orders may be traced and recovered.

12 The Order is made in exercise of the powers conferred under Proceeds of Crime Act 2002, ss.444 and 459(2).

13 An external request is a request by an overseas authority to prohibit dealing with property identified in the request: Proceeds of Crime Act 2002, s.447(1).

14 The relevant authority will be the Director of the National Crime Agency or the Director of Public Prosecutions and, in respect of offences involving serious or complex fraud or bribery, the Director of the Serious Fraud Office: Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005, Article 6.

15 Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005, Article 7.

© Law Business Research 2021

Where the Court is satisfied that these conditions are met, it may make a restraint order prohibiting a person from dealing with the property identified in the external request, subject to certain exceptions.[16] A restraint order must be served on the suspect and any other person affected by it, and the Court will require confirmation that this has been done.

It is likely that any banks or financial institutions in the United Kingdom to which the individual is connected will be served with a copy of the restraint order to freeze any assets (ensuring that they remain available for confiscation).

17.3.2 Account monitoring orders

CICA implemented the 2001 Protocol to the Convention on Mutual Assistance in Criminal Matters (the 2001 Protocol), which created obligations for participating countries to respond to requests from overseas authorities for assistance locating bank accounts or to provide banking information relating to criminal investigations.[17] The requirements of the 2001 Protocol now appear within Article 661 of the TCA in like terms. Account monitoring orders under CICA only apply to an investigation by a 'participating country' into serious criminal conduct.[18]

Account monitoring orders were first introduced in the United Kingdom under POCA. However, separate provisions were created under CICA to ensure that the United Kingdom could meet the wider requirements of the 2001 Protocol.

Where the SSHD receives a request from an overseas authority, they may direct a senior police officer to apply, or arrange for a constable to apply, for an account monitoring order.[19] A judge can make an account monitoring order for up to 90 days where satisfied that there is an investigation into criminal conduct in the country in question and that the order is sought for the purposes of that investigation.[20] Applications can be made, without notice, to a judge in chambers.[21] The court may discharge or vary an account monitoring order, but not on an application by the account holder.[22]

An account monitoring order can also be requested under Part 5 of the Proceeds of Crime (External Investigations) Order 2014 for the purposes of

16 ibid., Article 8.

17 Crime (International Co-operation) Act 2003, ss.32 to 36.

18 Participating countries for this purpose include Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United States.

19 An account monitoring order is made by a judge to enable transactions on a particular account to be monitored for a specified period: Crime (International Co-operation) Act 2003, s.35.

20 Crime (International Co-operation) Act 2003, s.36.

21 ibid.

22 ibid.

© Law Business Research 2021

a criminal investigation[23] or criminal proceedings.[24] The request must demonstrate reasonable grounds for believing that the account information requested is of substantial value to the overseas investigation, and that it is in the public interest for it to be provided.[25]

Confiscation and forfeiture 17.3.3

Under the 2005 Order, property within the United Kingdom may be subject to confiscation proceedings following the receipt of an external order.[26]

Upon receipt of an authenticated external order, the SSHD may refer it to the relevant UK authority[27] to process and make an application to the Crown Court.[28] The Court will give effect to an external order where certain conditions are met. Those conditions are that:

- the external order was made following a conviction of the person named in the order, and no appeal is outstanding;
- the external order is in force and there is no appeal outstanding;
- giving effect to the order would not be incompatible with the Convention rights[29] of the individual concerned; and
- the property is not subject to charges under the provisions set out in Article 21(6) of the 2005 Order.[30]

Where the Crown Court decides to give effect to an external order, it must register it and provide for notice of the registration to be given to any person affected by it, who may apply to vary the order so that it applies to different property.[31]

---

23 Provided that the investigation falls within a confiscation investigation or a civil recovery investigation.

24 Proceeds of Crime Act 2002,Part 8, .

25 Proceeds of Crime (External Investigations) Order 2014, Article 30, .

26 An external order is made by an overseas court where property is found, or believed to have been obtained, as a result of, or in connection with, criminal conduct: Proceeds of Crime Act 2002, s.447(2)(b).

27 The relevant authority will be the Director of the National Crime Agency or the Director of Public Prosecutions, and, in respect of offences involving serious or complex fraud or bribery, the Director of the Serious Fraud Office: Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005, Article 18.

28 ibid., Article 20.

29 The United Kingdom's ongoing commitment to the European Convention on Human Rights is set out in the UK–EU Trade and Cooperation Agreement, Article 524.

30 The fourth condition is that the specified property must not be subject to a charge under: Drug Trafficking Offences Act 1986, s.9; Criminal Justice Act 1988, s.78; Criminal Justice (Confiscation) (Northern Ireland) Order 1990, Article 14; Drug Trafficking Act 1994, s.27; or Proceeds of Crime (Northern Ireland) Order 1996, Article 32.

31 Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005, Article 22.

© Law Business Research 2021

Under Article 26 of the 2005 Order, the amount ordered to be paid is due on the date notice is given to the affected person. The Crown Court has discretion to allow for more time to pay.[32]

17.3.4 Interviews

See Chapter 15 on representing individuals in interviews

An individual suspected of criminal activity who is resident or present in the United Kingdom and whom the UK authorities wish to question in connection with a domestic investigation will be interviewed 'under caution'. This is usually done voluntarily unless it is considered necessary to arrest the individual and there are legitimate reasons for doing so.[33] The interview will be conducted in accordance with the procedures laid down in the Police and Criminal Evidence Act 1984 (PACE) and the accompanying Code C. The suspect has a number of rights, including the right to have a UK lawyer present.[34]

The question of whether the interview is admissible in proceedings in any other jurisdiction will depend on the laws of that country. This means that, in cross-border investigations, serious consideration must be given before any interview in the United Kingdom as to whether a suspect's answers (or silence) may be admissible in any other investigating jurisdiction and, if so, the appropriate strategy to adopt.

When a suspect is resident in the United Kingdom, but is wanted for questioning by an overseas authority, the individual (or their legal advisers) may be approached with a request that the suspect travel to the requesting state for interview voluntarily.

In the absence of any such request, or if it is refused, the requesting authority can request via MLA that a statement be taken from the suspect on a voluntary basis. Alternatively, where the evidence needs to be taken on oath, or where the suspect refuses to co-operate, the request can be for the suspect to be compelled to attend court for questioning. Once before the court, the suspect can be questioned under oath, but retains the right against self-incrimination and may refuse to answer any question.[35]

If a suspect consents to giving the overseas authority a statement voluntarily, or answers questions in court, this is likely to be admissible in any future proceedings in the requesting jurisdiction (subject to the applicable local law). Again, the question of whether statements are also admissible in proceedings in any other jurisdiction will depend on local laws, and serious consideration must be given to the implications.

---

32 ibid., Article 26.

33 Such as a reasonable belief that, unless placed under arrest, the suspect will abscond from the jurisdiction or will attempt to improperly interfere with the investigation: Police and Criminal Evidence Act 1984, s.24 and Code G.

34 Police and Criminal Evidence Act 1984, Code C, para. 6.

35 A person cannot be compelled to give any evidence before a court that they could not be compelled to give in criminal proceedings in the United Kingdom or in criminal proceedings in the requesting state: Crime (International Co-operation) Act 2003, Schedule 1, para. 5.

© Law Business Research 2021

Where the requesting state seeks to obtain evidence from a witness who is not a suspect in an investigation, the same MLA procedures can be used.

However, if it is believed that the witness will be unwilling to assist other than by compulsion, and assuming that the investigation is into a serious or complex fraud, or bribery or corruption, of the type that would fall under the remit of the Serious Fraud Office (SFO), an MLA request can be made to direct the SFO to obtain such evidence from the individual using its compulsory section 2 powers.[36] Answers obtained via this process (noting that a failure to comply with a compulsory power such as section 2 can amount to a separate criminal offence) are not generally admissible as evidence against the interviewee in criminal proceedings,[37] although they will inform the rest of the investigation.

Before granting the request, the requesting authority will be expected to provide an undertaking that any statement, or the contents of any interview, given by an individual pursuant to a compulsory section 2 notice will not be used in evidence against that person in any subsequent prosecution.[38]

Practitioners should also consider the potential use by other jurisdictions of information provided in the United Kingdom by witnesses pursuant to authorities' compulsory powers; for example, the use of compelled testimony, obtained in the United Kingdom, in criminal proceedings in the United States would likely amount to a breach of an individual's privilege against self-incrimination.[39]

Search and seizure 17.3.5

Under section 16 of CICA, an overseas authority can request the search or seizure of property in the United Kingdom. However, a request will not be granted automatically, even if a search warrant has been issued in the requesting country.

In the first instance, the UK authorities may choose to implement the request less invasively, such as by seeking the production of documents. Where the UK authorities accede to the request, an application must be made to the court for a warrant to be granted.

Under section 17 of CICA, a court in England and Wales may only issue a warrant at the request of an overseas authority if satisfied that (1) criminal proceedings have been instituted, or a person has been arrested during the course of a criminal investigation, outside the United Kingdom, (2) the offence at issue would constitute an indictable offence in England or Wales, and (3) there are reasonable grounds to suspect that the premises in question are occupied or controlled by that person and contain evidence relating to the offence.[40]

---

36 Criminal Justice Act 1987, s.2,. The Financial Conduct Authority has a similar power under the Financial Services and Markets Act 2000, s.171.

37 Answers given in compelled interviews will, however, be admissible against the interviewee in most types of non-criminal proceedings.

38 *Saunders v. The United Kingdom* [1996] ECHR 65, para. 68 in particular.

39 *United States v Allen* No. 16-898 (2d Cir. 2017).

40 Crime (International Co-operation) Act 2003, s.17(3).

© Law Business Research 2021

An application for a search warrant must be supported by a written document, known as an information, setting out the factual basis on which the warrant is sought. Since search warrant applications are made *ex parte*, the officer making the application must furnish the court with the full facts at their disposal (including those that militate against the granting of a warrant).[41]

Where a warrant is granted, an officer from the executing UK authority may enter the property to seize and retain the evidence particularised in the warrant. All search warrants executed in the United Kingdom must comply with the requirements of PACE and the accompanying Code B.[42] This includes a requirement to provide the occupier of the premises with a copy of the warrant. Failure to comply with the relevant requirements may leave the warrant vulnerable to challenge by way of judicial review.

Where evidence is seized under CICA, either the original or a copy will be sent via the UKCA to the requesting territory.[43] However, further considerations will apply in the event that the material seized is subject to legal professional privilege or constitutes 'special procedure material'.[44]

See Chapter 36 on privilege

An individual may, however, hold privileged material belonging not only to themselves, but also to their current or former employer (such as legal advice given to the company or material generated during an internal investigation).[45] If such material is seized, the company benefiting from the privilege may wish to make representations to the authority receiving the material.

17.3.6 Production of documents

See Chapter 11 on production of information to authorities

In cross-border investigations involving financial crime, the most common mechanism to compel individuals to provide information, whether by answering questions in interview or by producing documents, is through the SFO's powers under section 2 of the Criminal Justice Act 1987.[46]

In the recent case of *R (KBR Inc) v. Serious Fraud Office*,[47] the Supreme Court held that section 2 powers do not have extraterritorial effect; consequently, section 2 powers cannot be used to compel a foreign company that does not carry on business in the United Kingdom or have a UK presence to produce

41 *R (Energy Financing Team) v. Bow Street Magistrates' Court* [2006] 1 WLR 1317.

42 Police and Criminal Evidence Act 1984, s.15(6) specifies what a warrant should contain.

43 Crime (International Co-operation) Act 2003, s.9.

44 Special procedure material includes journalistic material, or material acquired or created in the course of any trade, business, profession or other occupation, which is held subject to a duty of confidentiality: Police and Criminal Evidence Act 1984, s.14.

45 The decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2018] EWCA Civ 2006 clarified the scope of material that might arguably be subject to legal professional privilege.

46 Equivalent powers exist under the Financial Services and Markets Act 2000, Part XI in respect of FCA investigations and Serious Organised Crime and Police Act 2005, s.62 in respect of National Crime Agency, HMRC and police investigations into 'specified offences'.

47 [2021] 2 WLR 335.

© Law Business Research 2021

documents held outside the country. However, the position in respect of documents held overseas may be different where the recipient of a section 2 notice is a UK-registered company or a foreign company with a presence in the United Kingdom or carrying on business in the United Kingdom, or where an individual's conduct abroad is concerned. Consideration should be given early in any cross-border investigation to what documents an individual possesses (whether in hard copy or electronically) and where they are held.

In addition, under section 20 of CICA, a participating country may request a freezing order in relation to evidence (this does not extend to property or money). Once evidence has been frozen it must be retained until instructions have been received to transfer that evidence to the requesting state, or to release it.[48]

Under the Crime (Overseas Production Orders) Act 2019, 'appropriate officers'[49] can apply to the Crown Court for an overseas production order[50] requiring a person based overseas in a country that is party to, or participates in, a 'designated international co-operation arrangement' to produce or give access to 'electronic data'[51] in his or her possession or control regardless of where it is stored. On 3 October 2019, the United Kingdom signed its first designated agreement with the United States pursuant to the US Clarifying Lawful Overseas Use of Data Act 2018.[52] This is the only country with whom the United Kingdom has signed a designated international co-operation agreement. However, the system is not yet fully operational.

Extradition 17.4

In cross-border criminal investigations, suspects are often resident outside the jurisdiction conducting the investigation.[53] As such, a critical question will be

48 Crime (International Co-operation) Act 2003, s.24.

49 The 'appropriate officers' include a constable, an officer of HMRC, a member of the SFO and a person appointed by the Financial Conduct Authority: Crime (Overseas Production Orders) Act 2019, s.2(1)(a).

50 The requirements of which the Crown Court judge must be satisfied before granting an overseas production order are set out in the Crime (Overseas Production Orders) Act 2019, s.4.

51 'Electronic data' is broadly defined within the Crime (Overseas Production Orders) Act 2019 as 'any data stored electronically', although Overseas Production Orders cannot require the production of material that is protected by legal professional privilege, or personal confidential records (s.3). Further, the agreement reached between the United Kingdom and United States limits the use of overseas production orders to those sought against 'communication service providers', defined in the agreement as an entity (or persons processing data on its behalf) providing certain services to the public, for example, big technology and social media companies providing a public platform for communications.

52 Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, USA No. 6 (2019).

53 The focus of this chapter is on extradition from the United Kingdom. However, individuals wanted by overseas authorities may be the subject of an Interpol red notice. Red notices can

© Law Business Research 2021

See Chapter 32 on extradition

whether, and how, they may be subjected to extradition. The answer lies in the legislation of, and arrangements between, the requesting and requested states.

Since the United Kingdom's exit from the European Union, extradition between the two is governed by Title VII to Part 3 of the TCA[54] and its obligations are implemented through the Extradition Act 2003 (the 2003 Act) as amended. The relevant 'surrender' provisions of the TCA replace the previous European Arrest Warrant (EAW) Framework but, for anyone arrested (or provisionally arrested) in the United Kingdom before 11pm on 31 December 2020 pursuant to an EAW, the extradition process will continue to follow the previous EAW Framework and the 2003 Act in its unamended form.[55] If an EAW was issued before 1 January 2021 but the requested person was not arrested before this date, the EAW will be treated as a Part 1 warrant as detailed below.

The 2003 Act is divided into two parts. Part 1 applies to requests made by 'category 1 territories' (EU Member States and Gibraltar) through the TCA procedure.[56] Part 2 applies to requests made by 'category 2 territories', namely those other countries with which the United Kingdom has extradition relations.[57]

17.4.1 Extradition from the UK – category 1 territories

Title VII to Part 3 of the TCA largely mirrors the EAW Framework and, therefore, Part 1 of the 2003 Act remains a fast-track procedure allowing the requesting state to secure the return of a requested person quickly and effectively.

The National Crime Agency certifies a Part 1 warrant on receipt from the requesting state before liaising with the Crown Prosecution Service (CPS) for advice on the validity and content of the request.

The requesting state must identify the offence or offences that the requested person is accused of committing and confirm that the Part 1 warrant is issued with a view to his or her arrest and extradition for the purpose of prosecution or, where the requested person has been convicted, for the purpose of being sentenced or

---

be issued on the basis that the individual is sought for prosecution or to serve a sentence. Once issued, a red notice alerts police and border officials around the world, and therefore affected individuals may encounter difficulties when travelling internationally, even if they are not subject to an investigation or arrest warrant in the jurisdiction they are travelling from or to. For more information, see https://www.interpol.int/INTERPOL-expertise/Notices/Red-Notices. Additionally, as a result of the Extradition (Provisional Arrest) Act 2020, the mere issuance of a red notice by Interpol at the request of Australia, Canada, Liechtenstein, New Zealand, Switzerland and the United States is now sufficient to warrant the arrest of the concerned individual in the United Kingdom.

54 Implemented domestically by the European Union (Future Relationship) Act 2020, the UK–EU Trade and Cooperation Agreement sets out the United Kingdom's extradition arrangements with the 27 EU Member States following the United Kingdom's departure from the previous European Arrest Warrant Framework.

55 *Polakowski v. Westminster* [2021] EWHC 53 (Admin).

56 Extradition Act 2003 (Designation of Part 1 Territories) Order (SI 2003/3333), as amended.

57 Extradition Act 2003 (Designation of Part 2 Territories) Order (SI 2003/3334).

© Law Business Research 2021

to serve a sentence already passed. The information must include details such as the requested person's identity and particulars of the alleged offence or conviction. Failure to comply with these requirements invalidates the Part 1 warrant.[58]

Following the certification of the Part 1 warrant, it may be executed and the requested person arrested[59] (provisional arrest may also be carried out if there are reasonable grounds for believing a Part 1 warrant has been or will be issued by a competent authority).[60]

On arrest, the individual will initially be taken to a police station and held there under the provisions of PACE and the accompanying Code C. The individual has various rights, including the right to have someone informed of the arrest, the right to free independent legal advice and the right to consult privately with a solicitor. A formal custody record will be opened, but the individual will not be interviewed as it is not the role of the police to investigate the offence. However, given the significance of identification to the extradition process, fingerprints, non-intimate samples and photographs may be obtained in accordance with PACE Code D.[61]

Following the requested person's arrest and initial detention, they must be brought before a court[62] 'as soon as practicable' for an initial hearing and fixing of the extradition hearing within the next 21 days.[63] Depending on the day and time of the arrest, this requirement can mean that the individual spends only hours in police detention before being brought before the court although, if arrested at the weekend, it can mean spending up to two nights in police custody.

At the extradition hearing, the judge must be satisfied that the alleged conduct constitutes an extraditable offence[64] and that no bar to extradition applies. If the judge orders extradition, and in the absence of any appeal, the requested person must be extradited within 10 days of the order, or later if agreed with the requesting state.[65]

Either party may appeal the judge's decision to the High Court.[66] Thereafter, an appeal may be made to the Supreme Court if the matter concerns a point of law of general public importance.[67]

58 Extradition Act 2003, s.2.

59 ibid., s.3.

60 ibid., s.5. A person subject to provisional arrest must be brought before the appropriate judge within 48 hours and an application for discharge must be granted if a certified warrant is not produced within that time frame: ibid., s.6.

61 ibid., ss.166 to 168.

62 In England and Wales, cases are heard at Westminster Magistrates' Court.

63 Extradition Act 2003, ss.4 and 8.

64 ibid., ss.64 and 65.

65 ibid., s.35.

66 ibid., ss.26 to 29.

67 ibid., s.32.

© Law Business Research 2021

17.4.2 Extradition from the UK – category 2 territories

Part 2 of the 2003 Act provides for the extradition to those territories not in category 1 with which the United Kingdom has bilateral or multilateral extradition treaties.[68] These territories are usually required to provide *prima facie* evidence of the case against the requested person unless they are signatories to the European Convention on Extradition,[69] or the United States, New Zealand, Australia or Canada.

If a requested person's extradition is sought so that the person stands trial, the request must be certified by the SSHD as being valid before being sent to the appropriate judge.[70] The judge then considers whether there are reasonable grounds to issue an arrest warrant,[71] which include that the evidence produced would justify the issue of a warrant for the individual's arrest if it were a domestic case.[72]

Once an arrest warrant has been issued and executed, the requested person must be brought before the magistrates' court as soon as practicable.[73] Unless the requested person consents to extradition, the court will fix a date for the extradition hearing, usually within two months, and decide whether to grant bail.[74]

At the extradition hearing, the judge must first consider the sufficiency of the extradition request and supporting documentation. If the documents do not meet the requirements set out in section 78(2) of the 2003 Act, the judge must discharge the person whose extradition is sought.[75] Where the judge is satisfied that the requirements have been met, they will consider whether the person before the court is the requested person, the offences specified are extraditable and copies of the documents have been served on the person.[76] In cases where *prima facie* evidence must be provided, the judge must then decide if the evidence supporting the request is 'sufficient to make a case'.[77]

---

68 A list of category 2 territories is provided at https://www.gov.uk/guidance/extradition-processes-and-review.

69 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024/signatures?module=signatures-by-treaty&treatynum=024.

70 Extradition Act 2003, ss.69 and 70.

71 ibid., s.71.

72 ibid., ss.137 and 138.

73 ibid., s.71.

74 A defendant in extradition proceedings has the right to bail unless alleged to be unlawfully at large after a conviction in the requesting territory: Extradition Act 2003, s.198. However, the usual grounds for refusing bail under the Bail Act 1976 apply together with an additional ground of refusal where the conduct constituting the extradition offence is an offence under UK law and appears to have been committed while the defendant was on bail.

75 Extradition Act 2003, s.78.

76 ibid.

77 ibid., s.84(1). This requires the judge to have regard to all the admissible evidence before the court, including evidence called by the requested person, to determine whether the judge is satisfied that there is evidence upon which the requested person could be convicted at

© Law Business Research 2021

If the judge is satisfied that all the conditions have been met, and that no bars to extradition exist, the matter is referred to the SSHD for a decision whether to extradite. Representations may be made by the requested person to the SSHD for consideration.

The judge's decision to refer may be appealed within 14 days of the date of the decision and thereafter appeals may be lodged with the High Court or, if appropriate, the Supreme Court.

Extradition from the UK – other territories 17.4.3

For countries that are neither category 1 nor category 2 territories, section 194 of the 2003 Act allows the SSHD to certify that 'special extradition' arrangements have been made between the United Kingdom and that country for the extradition of a person. These special arrangements must comply with the 2003 Act's Part 2 procedures.

In addition, a territory party to an international convention to which the United Kingdom is also a party may, under section 193, be designated a territory to which Part 2 applies.[78]

Bars to extradition 17.4.4

Under the 2003 Act, a properly issued extradition request will be honoured, unless one of the bars to extradition applies.

Sections 11 and 79 of the 2003 Act set out specific bars to extradition for Part 1 and Part 2 requests, respectively. These include the rule against double jeopardy, extraneous considerations and the passage of time.

In addition to the specific bars, there are a number of general bars, as detailed below.

The human rights bar 17.4.4.1

Under sections 21, 21A (Part 1 cases) and 87 (Part 2 cases), the judge must determine 'whether extradition would be compatible with the requested person's Convention rights' within the meaning of the Human Rights Act 1998.[79] A request may be refused where it is shown that there are substantial grounds to believe that the requested person, if extradited, faces a 'real risk of exposure to inhuman or degrading treatment or punishment'[80] contrary to Article 3 of the European Convention on Human Rights (ECHR) (for example, in relation

---

a 'summary trial of an information' against the person: *Devani v. Republic of Kenya* [2015] EWHC 3535 (Admin).

78 The Extradition Act 2003 (Parties to International Conventions) Order 2005 provides that a state will only be designated a category 2 territory in this way in relation to conduct to which the convention applies, e.g., drug trafficking offences in contravention of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

79 Extradition Act 2003: ss.21(1) and 21A(1)(a) (Part 1 cases) and s.87(1) (Part 2 cases).

80 *Soering v. United Kingdom* (1989) 11 EHRR 439.

© Law Business Research 2021

to prison conditions in the requesting state); or that the interference with the private and family lives of the requested person, and members of his or her family, outweighs the public interest in extradition.[81] Arguments under Article 5 (the right to liberty and security)[82] and Article 6 (right to a fair trial)[83] of the ECHR can also be raised under the human rights bar.

17.4.4.2 The proportionality bar

This bar applies to Part 1 cases only.[84] When considering a request, the judge may consider the seriousness of the alleged conduct, the likely penalty to be imposed and whether there are alternatives to extradition.

17.4.4.3 The forum bar

The forum bar provides that extradition may be barred if it would not be in the interests of justice.[85] This will be considered where the nature of the criminal conduct means that the alleged offence could potentially be prosecuted in more than one country, and is particularly relevant to parallel or cross-border investigations. It was introduced into the 2003 Act by the Crime and Courts Act 2013 as a result of concern, in particular in the context of extraditions to the United States, and has been in force as a bar to extradition since October 2013.

Extradition would not be in the interests of justice if the judge decides that a substantial measure of the criminal activity took place in the United Kingdom having regard to 'specified matters'. The specified matters include consideration of:

- where most of the loss or harm occurred or was intended to occur;
- the interests of any victims;
- any belief of a prosecutor that the United Kingdom is not the most appropriate jurisdiction in which to prosecute;
- desirability and practicability of all prosecutions relating to the extradition offence taking place in one jurisdiction;
- and the requested person's connections with the United Kingdom.[86]

The forum bar has been successfully invoked on several occasions concerning extradition to the United States (*Love*, *Scott*, *McDaid* and *Taylor*)[87] but the court

81 *HH v. Deputy Prosecutor of the Italian Republic, Genoa* (2012) 3 WLR 90 summarised the conclusions of Baroness Hale re: case law interpreting Article 8 of the European Convention on Human Rights.

82 *Shankaran v. India* (2014) EWHC 957 (Admin).

83 *Vincent Brown aka Vincent Bajinja, et al. v. The Government of Rwanda, The Secretary of State for the Home Department* (2009) EWHC 770 (Admin).

84 Extradition Act 2003, s.21A.

85 ibid., s.19B (Part 1 cases) and s.83A (Part 2 cases).

86 ibid., s.19B(3) (Part 1 cases) and s.83A(3) (Part 2 cases).

87 *Love v. Government of the United States and another* [2018] EWHC 172 (Admin), *Scott v. Government of the United States of America* [2018] EWHC 2021 (Admin), *United States*

© Law Business Research 2021

has more recently rejected a forum bar argument advanced in the high-profile extradition proceedings relating to Mike Lynch, who is sought for trial in the United States in relation to fraud charges (although this decision is subject to appeal).

Settlement considerations 17.5

The scope for an individual to settle cross-border investigations or proceedings is in practice limited and will realistically arise either in circumstances where the individual can obtain an immunity from prosecution or where his or her co-operation in one jurisdiction (whether or not involving a guilty plea) effectively resolves the investigations in other jurisdictions.

Sections 71 to 75 of the Serious Organised Crime and Police Act 2005 set out the statutory framework in which an individual may enter into such an agreement with a UK prosecutor.[88]

Under section 71, a designated prosecutor[89] may grant a suspect immunity from prosecution subject to certain conditions which, if breached, will ordinarily result in the immunity being revoked. These conditions invariably require a suspect's full co-operation with the prosecuting authority in the United Kingdom (and, where applicable, with overseas authorities).

Whereas section 71 grants immunity from prosecution, section 73 requires an individual to plead guilty to the offence, but enables the court to take into consideration the assistance the individual has provided to the authorities. This will often result in a substantial reduction in sentence.[90] A section 73 agreement is often referred to as a 'co-operating defendant' agreement and, in practice, in cross-border investigations will require the individual to co-operate also with overseas authorities.

Unlike in other jurisdictions, a deferred prosecution agreement (DPA) can only be concluded between the SFO or CPS[91] and a suspect corporate entity; there is no provision for an individual to enter into a DPA.[92] The use to which the SFO or CPS can put the information it obtains during the DPA negotiations against others, including individuals employed by the corporate entity, is

v. McDaid [2020] EWHC 1527 (Admin) and *Government of the United States of America v. Taylor*.

88 In this context, 'the United Kingdom' refers to England, Wales and Northern Ireland.

89 Defined by the Serious Organised Crime and Police Act 2005, s.71(4), as a prosecutor from the CPS, HMRC, SFO or the Director of Public Prosecutions of Northern Ireland.

90 *R v. Dougall* [2010] EWCA Crim 1048.

91 The SFO and the CPS are currently the only authorities authorised to enter into DPAs: Crime and Courts Act 2013, Schedule 17, para. 3(1).

92 Crime and Courts Act 2013, Schedule 17, para. 4(1).

© Law Business Research 2021

unrestricted.[93] This means that an employee suspect is at risk of having his or her position compromised as a result of the employer's co-operation.[94]

If a corporate entity with which the client is connected enters into a DPA, the client may be named in the published statement of facts that underpins the DPA. A third party does not have to be notified that he or she may be so named and the terms of a DPA and the supporting statement of facts cannot be altered or modified once approved by the court.[95]

If there are existing or anticipated criminal proceedings against individuals, relevant names will be anonymised, or restrictions will be imposed on the publication of the statement of facts,[96] to avoid the risk of the DPA causing prejudice to those proceedings.

17.6 Reputational considerations

Throughout parallel or cross-border investigations or proceedings, those representing an individual must always consider the potential impact on the client's reputation. Matters are complicated where the individual may have a low profile in one jurisdiction, but be well known in another, or, despite having a low media profile, may have become embroiled in a highly public investigation.

Associated issues can arise where the individual is included in a due diligence database, such as World Check or World Compliance. Entry in these databases, which are largely based on open source (and sometimes unreliable) material, can have a profound effect on an individual's ability to access financial services, but representations can sometimes be made to seek to amend a client's profile.

As regards criminal investigations, the UK courts have affirmed that, as a starting point, a suspect should not be named by the press.[97] However, in the context of cross-border investigations, different jurisdictions will have different rules on publishing a suspect's identity such that an individual who avoids having their details published by the UK press may nevertheless find themselves named overseas. Furthermore, different considerations will apply where, for example, an individual is charged in a criminal investigation (as opposed to being merely under suspicion) or, in the context of FCA proceedings, 'identified' in corporate decision notices.[98]

---

93 ibid., Schedule 17, para. 13(6).

94 In trying to put itself into a position where it can reach a DPA, the corporate entity will be anxious to demonstrate its co-operation with the concerned authority. Co-operation is a public interest factor militating against prosecution under the joint SFO and CPS Code of Practice: DPA Code of Practice, para. 2.8.2(i), Crime and Courts Act 2013.

95 *SFO v. Tesco Stores Limited* [2019] EW Misc 1 (Crown C), para. 4.

96 For example, the DPA in *SFO v. Sarclad Limited* [2016] Lloyd's Rep FC 509 (formerly referred to as *SFO v. XYZ Ltd).*

97 *Richard v. The British Broadcasting Corporation (BBC) & Anor* [2018] EWHC 1837 (Ch), paras. 248–51; and *ZXC v. Bloomberg* [2020] EWCA Civ 611, paras. 81–84.

98 *Financial Conduct Authority v. Macris* [2017] UKSC 19.

© Law Business Research 2021

18

Individuals in Cross-Border Investigations or Proceedings: The US Perspective

Amanda Raad, Michael McGovern, Meghan Gilligan Palermo, Zaneta Wykowska, Abraham Lee and Chloe Gordils[1]

Introduction 18.1

There has been a consistent trend in the United States in the past decade towards increased prosecution of individuals in white-collar cases, including for financial fraud and foreign corruption offences. Following widespread criticism after the 2008 financial crises for failing to criminally charge individual wrongdoers, the US Department of Justice (DOJ) implemented a policy shift towards individual accountability, focusing on prosecuting individuals responsible for corporate misconduct and financial fraud.[2]

Even during the covid-19 pandemic, the DOJ and the Securities and Exchange Commission (SEC) continued to focus on prosecuting and charging individuals in white-collar cases.[3] In 2020, the DOJ Criminal Division's Fraud

1 Amanda Raad and Michael McGovern are partners, and Meghan Gilligan Palermo, Zaneta Wykowska, Abraham Lee and Chloe Gordils are associates, at Ropes & Gray LLP.

2 Beginning with the Yates Memorandum (Yates Memo), issued in late 2015 by former US Dep. Att'y Gen.l Sally Yates, the Department of Justice (DOJ) instituted a policy emphasising the need for US prosecutors to pursue prosecutions of individuals involved in corporate wrongdoing. To effectuate this policy, the Yates Memo mandated that, for a company to receive any co-operation credit, it must provide the DOJ with 'all relevant facts about the individuals involved in corporate misconduct' in both criminal and civil cases, regardless of the level of their involvement in the alleged misconduct. See Memorandum from Sally Quillian Yates, Dep. Att'y Gen., DOJ, Individual Accountability for Corporate Wrongdoing (9 Sep. 2015), https://www.justice.gov/dag/file/769036/download.

3 In recent years, the DOJ has relaxed the rigid requirements of the Yates Memo, no longer requiring companies to identify every person with a role in wrongdoing, regardless of culpability level. However, DOJ policy still mandates that companies identify all individuals who were 'substantially involved in or responsible for the misconduct at issue' to receive

© Law Business Research 2021

Section charged 326 individuals, compared with 478 in 2019.[4] And as with the ever-increasing globalisation of the world economy, white-collar enforcement against individuals is increasingly cross-border.[5]

For American white-collar practitioners, this means representing clients in all corners of the world as they navigate cross-border criminal prosecutions, civil enforcement actions and corporate internal investigations. Although there are important distinctions unique to each, many of the issues discussed in this chapter are common to all three. Counsel representing overseas clients will

---

any co-operation credit. In the civil context, the DOJ has implemented a 'sliding scale' approach where co-operation credit is awarded based on the degree of co-operation. See Rod J Rosenstein, Dep. Att'y Gen., DOJ, Prepared Remarks for the 35th International Conference on the Foreign Corrupt Practices Act (29 Nov. 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0. In addition, in updated guidance issued in June 2020, the DOJ promulgated further guidelines concerning how companies should monitor the conduct of individual employees and how the behaviour of those employees intersects with the DOJ's evaluation of a company's compliance programme for purposes of assessing co-operation credit. See DOJ, Criminal Division, 'Evaluation of Corporate Compliance Programs' (Jun. 2020) (the Guidance). The Guidance places greater emphasis on how effectively a company's compliance programmes are communicated to employees, as well as on how the company tracks and monitors their behaviour. For example, the Guidance provides that prosecutors evaluating a company's compliance programme must consider whether (1) the company's policies and procedures have been made easily accessible to employees, (2) employees are appropriately trained and given the opportunity to raise questions, (3) the company has addressed employees who fail all or a portion of testing on compliance policies, (4) the company has evaluated the extent to which training has had an impact on employee behaviour or operations, (5) the company takes measures to test employees' awareness of and comfort using reporting mechanisms such as hotlines, and (6) the compliance function monitors investigations and discipline to ensure consistency. These additions to the Guidance suggest that where a company has implemented effective measures to address each of the foregoing questions, the DOJ will look even more critically at individual employees who circumvent the company's controls. The updated Guidance also makes explicit that the DOJ expects a culture of ethics and compliance at all levels of the company, including middle-management.

4 Compare DOJ, Criminal Division Fraud Section Year in Review 2020, https://www.justice.gov/criminal-fraud/file/1370171/download, with DOJ, Criminal Division Fraud Section Year in Review 2019, https://www.justice.gov/criminal-fraud/file/1245236/download.

5 For example, in a headline case in 2020, the DOJ charged 28 North Korean bankers for helping launder more than US$2.5 billion out of the sanctioned country to pay for Pyongyang's nuclear weapon and missile programme. The indictment charges the individuals with international money laundering, bank fraud and violations of the International Emergency Economic Powers Act, and alleges an intricate scheme that involved creating secret branches of a state-owned bank in countries such as China, Russia, Libya and Thailand. See *U.S. v. Man, et al.*, Indictment, No. 1:20-CR-00032, https://int.nyt.com/data/documenthelper/6971-north-korea-indictment/422a99ddac0c39459226/optimized/full.pdf#page=1 (5 Feb. 2020).

© Law Business Research 2021

need to consider a host of additional issues, including jurisdiction, extradition and collateral consequences, to name a few.

Preliminary considerations 18.2

Arrest and bail 18.2.1

The first critical issue counsel face in criminal proceedings is counselling a client through arrest and bail. US authorities have various means for apprehending criminal defendants,[6] including arrest in the United States, arrest in a foreign jurisdiction and extradition to the United States, or using Interpol red notices to detain foreign individuals travelling abroad.[7] If a client is arrested abroad, counsel should immediately arrange for experienced local counsel. The availability of provisional arrest and bail pending extradition will depend on the laws of the arresting jurisdiction.

Arrest in the United States presents its own difficulties. Counsel will need to arrange for the client to appear in US court and apply for bail.[8] In most cases, an overseas client will naturally wish to return home pending proceedings in the United States. However, the client's foreign status may be the very thing that makes it difficult to obtain a bail package allowing international travel. The court is more likely to find that the client poses a flight risk (i.e., a risk of fleeing the jurisdiction to avoid criminal prosecution) due to limited US ties. This concern is greater where the client has substantial financial resources or ties to a country that has not entered into an extradition treaty with the United States.[9] Counsel should discuss these risks with the client and obtain a complete understanding of his or her financial and personal circumstances to

6 See DOJ, Justice Manual § 9-15.635 (2018), https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters (Justice Manual); see also DOJ, Justice Manual: Criminal Resource Manual § 611 (2020), https://www.justice.gov/jm/criminal-resource-manual-601-699 (Criminal Resource Manual).

7 For this reason, counsel engaged during the investigatory phase of a cross-border DOJ investigation should carefully consider the client's exposure to prosecution and risk of arrest while overseas. The client should be advised to carry counsel's contact details at all times. In some cases, and taking into consideration the client's home country, counsel may advise the client to refrain from international travel while the DOJ's investigation is pending.

8 Under the Bail Reform Act, 18 U.S.C. § 3142(b) & (c)(1)(B), US courts must order a defendant's pretrial release unless the court 'determines that such release will not reasonably assure the appearance of the person as required or will endanger the safety of any other person or the community.' Where a defendant is released, the court must do so 'subject to the least restrictive further condition, or combination of conditions that . . . will reasonably assure the appearance of the person'. On the other hand, a court must order detention if it 'finds that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community'. Id. § 3142(e).

9 See, e.g., *United States v. Zarrab*, 15-CR-867, 2016 WL 3681423, at *7 (S.D.N.Y. 16 Jul. 2016); *United States v. Epstein*, 155 F. Supp. 2d 323, 326 (E.D. Pa. 2001).

© Law Business Research 2021

submit a bail application that mitigates flight-risk concerns.[10] Even if pretrial release is granted, courts commonly impose a stringent set of conditions to guarantee the defendant's ongoing appearance. These conditions may include, for example, home confinement, restrictions of travel to certain countries or districts within the United States, confiscation of travel documents and electronic monitoring.

18.2.2 Preservation of evidence and maintaining confidentiality

Counsel must promptly ascertain whether the client has physical evidence relating to the matter in question. This may include emails, hard drives, text and instant messaging, financial records, and documentary evidence. Counsel should advise clients of the obligation to preserve and not destroy evidence, and consider whether to proactively collect and review such data.

Counsel will likewise need to preserve the integrity of the client's factual recollection. This includes assessing whether the client has discussed relevant matters with potential co-defendants or other parties. Clients should be advised not to communicate with any third parties regarding the matters under investigation and, in most cases, to cease communications with co-defendants entirely.[11]

18.2.3 Initial conversations with the client

Counsel should meet with the client to assess the facts and available evidence as quickly as possible. These early conversations will inform counsel's strategy for reviewing evidence, pursuing additional lines of inquiry, assessing strategic

10 Nevertheless, with the onset of the covid-19 pandemic, US courts have appeared more willing to grant bail to foreign defendants where the defendant is able to show pre-existing health conditions that place him or her at heightened risk of dangerous health-related complications. See, e.g., *In re Manrique*, No. 3:19-mj-71055'MAG (N.D. Cal. 19 Mar. 2020) (granting bail to 74-year-old former president of Peru arrested on an extradition warrant issued by Peru for bribery in connection with the Odebrecht scandal pending resolution of the extradition case owing to his increased vulnerability to covid-19 as a result of age and other factors).

11 Communications with such parties should be through counsel and only pursuant to common interest privilege.

© Law Business Research 2021

options, identifying potential common interest discussions[12] and determining what resources are needed,[13] such as specialised counsel.[14]

Extradition 18.3

It is of increasing importance that counsel representing individuals in cross-border proceedings have, at a minimum, working knowledge of extradition law given the frequency with which extradition issues arise. In recent years, the United States has aggressively pursued extradition, including in white-collar cross-border proceedings involving Foreign Corrupt Practices Act (FCPA), money laundering, and securities and commodities law violations.[15] However, the covid-19 pandemic resulted in temporary delays to the execution of international arrest warrants and extraditions in 2020 owing to travel restrictions and court closures, and saw many matters resuming via videoconference rather than in court appearances.[16]

See Chapter 32 on extradition

12 See id.

13 Initial discussions with the client should include a detailed and candid conversation about the client's financial resources, goals for how those resources are deployed and the availability, if any, of insurance coverage. Litigating criminal actions has grown increasingly expensive in recent decades. Counsel should ensure that the client has a complete understanding of the resources necessary to defend the case, particularly if the client fights the charges and all the more so if the client is self-funding the representation. Where a client is able to be covered under a directors and officers (D&O) policy or similar liability insurance, counsel may advise the client to retain specialised insurance counsel to assist in obtaining and understanding potential limitations on coverage, for example, policy provisions allowing the insurer to claw back legal fees if the client later pleads or is found guilty of criminal charges.

14 In all cases, it is important to consider at the outset the need for other counsel, including employment counsel, extradition counsel, regulatory counsel or counsel specialising in the privacy laws of the relevant jurisdiction.

15 Bruce Zagaris, *International White Collar Crime: Cases and Materials*, 413 (2d ed. 2015), ('According to the Department of State, US courts certified 137 extradition requests between 1945 and 1960 – an average of only 9 per year. In 1995, in contrast, the US extradited 79 people to other countries and received custody of 131').

16 For example, in March 2020, extradition proceedings against WikiLeaks founder Julian Assange, who is currently facing conspiracy and espionage charges by US authorities relating to the leak of classified documents, were postponed because of a coronavirus lockdown in the United Kingdom and resumed in September 2020 via videoconference, but they were marred by several technical difficulties. See Megan Specia, 'At Assange's Extradition Hearing, Troubled Tech Takes Center Stage', *New York Times* (16 Sep. 2020), https://www.nytimes.com/2020/09/16/world/europe/assange-extradition-hearing.html. Although the district judge ruled that Assange should not be extradited to the United States in light of mental health concerns in January 2021, the ruling is under appeal. See Alistair Smout, 'U.S. Tries Again to Extradite Wikileaks' Assange from Britain,' Reuters (11 Aug. 2021), https://www.reuters.com/world/us-tries-again-extradite-wikileaks-assange-britain-2021-08-11/.

© Law Business Research 2021

18.3.1 Applicable law

The US government often is able to secure the presence of a criminal defendant for trial only with the assistance of foreign authorities. While there are technically no limitations on US authorities' ability to seek extradition of individuals abroad, the United States typically does so through extradition requests made pursuant to a treaty.

Extradition treaties form the basis for extradition law and procedure. Signatory states agree to extradite individuals within their jurisdiction who have been charged with an extraditable offence to the requesting state for trial and punishment.[17] Each treaty specifically defines which offences are 'extraditable'.[18] Most modern treaties permit extradition where the alleged conduct is criminal and punishable as a felony in the signatory states (the 'dual criminality' approach).[19] Treaties may also specify which offences are not extraditable, for example military offences or those punishable by death.[20] Other common provisions include prohibitions on double jeopardy, limitation periods and restrictions on the extradition of nationals.[21]

17 See Ronald J Hedges, Federal Judicial Center International Litigation Guide: International Extradition: A Guide for Judges 1, 4 (2014), https://www.fjc.gov/sites/default/files/2014/International-Extradition-Guide-Hedges-FJC-2014.pdf.

18 For instance, the treaty between Albania and the United States includes an inventory of more than two dozen crimes. Extradition Treaty, Alb.-U.S., art. 2 (1 Mar. 1933), 49 Stat. 3313.

19 Justice Manual, supra note 6, § 9-15.635 (2018); see also Criminal Resource Manual, supra note 6, § 603.

20 See, e.g., Extradition Treaty, U.K.-U.S., art. 4(1)-(2) (31 Mar. 2003), T.I.A.S. 07-426 (UK Extradition Treaty).

21 Historically, the most common extradition treaty provision provided that signatory countries were not required to extradite their own citizens. See M Cherif Bassiouni, *International Extradition: United States Law and Practice*, 746 (6th ed. 2014). This practice has evolved, however, and many modern treaties contain provisions either prohibiting signatory countries from denying extradition on the basis of nationality, or providing that denial on the basis of nationality is permissible only if the case is referred to local authorities for prosecution. See, e.g., UK Extradition Treaty, supra note 20, art. 3; Extradition Treaty, Peru–U.S., art. 3, 26 July 2001, T.I.A.S. 03-825; Extradition Treaty, Belize–U.S., art. 3, 30 March 2000, T.I.A.S. 13089; Extradition Treaty, Para.–U.S., art. 3, 9 November 1998, T.I.A.S. 12995; Extradition Treaty, S. Kor.–U.S., art. 3, 9 June 1998, T.I.A.S. 12962; Extradition Treaty, Pol.–U.S., art. 4, 10 July 1996, T.I.A.S. 99-917. Certain countries, however, continue to prohibit extradition of their nationals but retain the discretion to do so. See, e.g., Extradition Treaty, Fr.–U.S., art. 3(1), 23 April 1996, T.I.A.S. 02-201 (France Extradition Treaty); Extradition Treaty, Ger.–U.S., art. 7(1), 20 June 1978, 32 U.S.T. 1485.

© Law Business Research 2021

To date, the United States has bilateral extradition treaties with approximately two-thirds (over 100) of the world's nations[22] and is party to two multilateral extradition agreements.[23]

Extradition procedure 18.3.2

Extradition procedure is determined by treaty, the responding state's extradition laws, and considerations of diplomacy and foreign policy. Typically, US authorities must first obtain approval from the DOJ's Office of International Affairs (OIA).[24] The OIA advises prosecutors regarding what filings are required under the applicable treaty, and the US Department of State issues a formal request to the responding state.[25] The responding state's judiciary then determines whether extradition is permissible.[26]

The US government may also seek provisional arrest, namely a request to the responding state to arrest the individual pending submission of a formal

22 See U.S. Dep't of State, Treaties in Force: A List of Treaties and Other International Agreements of the U.S. in Force on January 1, 2020, https://www.state.gov/wp-content/uploads/2020/08/TIF-2020-Full-website-view.pdf (Treaties in Force 2020); U.S. Dep't of State, Treaties in Force: Supplemental List of Treaties and Other International Agreements (2021), https://www.state.gov/wp-content/uploads/2021/05/TIF-Supplement-2021-website-view.pdf (Treaties in Force 2021 Supplement).

23 See Inter-American Convention on Extradition, 26 December 1933, 49 Stat. 3111, https://avalon.law.yale.edu/20th_century/intam04.asp, European Union–U.S., 25 June 2003, S. Treaty Doc. No. 109-14, https://www.congress.gov/109/cdoc/tdoc14/CDOC-109tdoc14.pdf. In addition, the United States is party to several multilateral international conventions that further reinforce bilateral extradition treaties by binding Member States to either extradite or prosecute individuals charged with particular offences. See, e.g., United Nations Convention for the Suppression of Unlawful Seizure of Aircraft art. 8, 16 December 1970, 860 U.N.T.S. 105; United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances art. 6 (20 Dec. 1988), 1582 U.N.T.S. 95.

24 Justice Manual, supra note 6, § 9-15.210.

25 id. § 9-15.300.

26 Specifically, the presiding judge in the foreign jurisdiction will confirm the identity of the individual, that the relevant treaty and domestic laws support extradition for the alleged offence, that the complaint filed by the United States sets forth sufficient facts to support probable cause to believe that the alleged offence was committed, and that all other elements of the extradition request comply with treaty provisions. See Hedges, supra note 17, at 10–11. The individual is then provided an opportunity to challenge the validity of the extradition request on various factual and procedural grounds. The Federal Rules of Criminal Procedure, Civil Procedure and Evidence do not apply in extradition proceedings. See *In re Requested Extradition of Kirby*, 106 F.3d 855, 867 (9th Cir. 1996) (Noonan J, dissenting); Fed. R. Evid. 1101(d)(3); Fed. R. Crim. P. 1(a)(5). Accordingly, hearsay evidence and unsworn statements may be admissible. See, e.g., *Haxhiaj v. Hackman*, 528 F.3d 282, 292 (4th Cir. 2008); *Zanazanian v. United States*, 729 F.2d 624, 626 (9th Cir. 1984); *Collins v. Loisel* (*Collins II*), 259 U.S. 309, 317 (1922); *Artukovic v.* Rison, 784 F.2d 1354, 1356 (9th Cir. 1986).

© Law Business Research 2021

extradition request.[27] The DOJ deems provisional arrests appropriate where there is a risk that the individual will flee the foreign jurisdiction.[28] The conditions under which provisional arrest is permissible, and the duration an individual may be held until a formal request is filed,[29] vary by treaty.[30]

The timeline for extradition to the United States varies depending on the circumstances of the case and the responding state involved.[31] Before the covid-19 pandemic, it took, on average, more than a year from the time the formal request was made until the individual was surrendered to US authorities.[32] Although many jurisdictions have expanded the use of live video and audio links so that certain extradition proceedings can continue remotely,[33] covid-19 related delays prolonged the extradition process for many defendants extending into early 2021.[34] While US courts have held that the Speedy Trial Clause of the Sixth Amendment requires that extradition be sought as soon as the individual's location becomes known,[35] this has no bearing on how long it

27 All modern US extradition treaties include articles providing for provisional arrest. See S. Exec. Rep. No. 106-26, at 31 (2000) (report from US Senate Committee on Foreign Relations); see, e.g., Extradition Treaty, Canada–U.S., art. 11(1), 3 December 1971, 27 U.S.T. 983.

28 Criminal Resource Manual, supra note 6, § 615.

29 Typically, once a provisional arrest is made, prosecutors have between one and three months to submit a formal extradition request. See Justice Manual, supra note 6, §§ 9-15.210, 9-15.230; see, e.g., Extradition Treaty, Canada–U.S., art. 11(1), 3 December 1971, 27 U.S.T. 983 (requiring release 'upon the expiration of forty-five days from the date of his arrest' if an extradition request is not received within that time).

30 If a client is taken into custody under a provisional arrest warrant, counsel likely will need to advise the client regarding bail, which may be sought in the responding jurisdiction while extradition is pending. Clients may need to mobilise significant resources and assemble bond guarantors to effectuate bail as quickly as possible. For this reason, too, it is essential that experienced extradition counsel in the relevant jurisdiction be engaged to navigate bail issues in the responding state.

31 Justice Manual, supra note 6, § 9-15.400.

32 Jonathan Masters, 'What is Extradition?, Counsel on Foreign Relations' (11 Apr. 2019), https://www.cfr.org/backgrounder/what-extradition.

33 For example, under the UK's Coronavirus Act 2020, courts have discretion to proceed with extradition hearings by video or audio links, subject to certain safeguards, if it is in the interests of justice to do so. See Coronavirus Act 2020, c.7 §§ 53–57.

34 For example, while Westminster Magistrates' Court (where all extradition proceedings in England and Wales are conducted) remained open for priority matters during much of the pandemic, with many requested persons appearing over video link, in some cases extradition hearings were adjourned for up to five months. See Joshua Kern and Lucia Brieskova, 'Prison Conditions and Extradition Proceedings In The Time Of Coronavirus', Crimeline (16 June 2020), https://crimeline.co.uk/knowledge-base/prison-conditions-and-extradition-proceedings-in-the-time-of-coronavirus/ (Kern and Brieskova, Prison Conditions and Extradition).

35 *United States v. Blanco*, 861 F.2d 773, 780 (2d Cir. 1988), cert. denied, 489 U.S. 1019 (1989); *United States v. Pomeroy*, 822 F.2d 718, 720 nn. 3–4 (8th Cir. 1987); *United States v. Walton*, 814 F.2d 376, 380 (7th Cir. 1987); see also Criminal Resource Manual, supra note 6, § 601–99.

© Law Business Research 2021

takes the responding state to surrender the individual according to its laws or due to other considerations.[36]

Strategic options: litigating or waiving extradition 18.3.3

Key factors affecting the decision to litigate or waive extradition include the following:

- *Strength of available extradition defences*: The advisability of litigating extradition turns primarily on whether it can be resisted successfully. While there are several defences available to extradition, they are limited.
- *Strength of evidence in the US criminal case*: The strength of US authorities' evidence of the charged crimes is also relevant. If the evidence is strong and there may be viable extradition defences, attempting to defeat extradition may be the best (and perhaps only) way to avoid liability on the criminal charges.[37] If, however, the evidence is strong and there are no viable or weak extradition defences, it is advisable to consider how best to mitigate eventual liability in the United States, including by considering consent to extradition in the hope of obtaining a favourable plea offer and sentence.[38] On the

36 For example, extradition proceedings in the foreign jurisdiction may be susceptible to political considerations, which may influence the timeline for extradition and even whether it occurs at all. The US government's ongoing effort to extradite WikiLeaks founder Julian Assange from the United Kingdom is a prime example. Current political uncertainties may have ultimately affected whether Mr Assange is extradited to the United States. See John T Nelson, 'L'Affaire d'Assange: Why His Extradition May Be Blocked', Just Security (7 Jun. 2019), https://www.justsecurity.org/64425/laffaire-dassange-why-his-extradition-may-be-blocked/. On 4 January 2021, the district judge overseeing the Assange trial ruled against the US government, finding that extradition to the United States 'would be oppressive by reason of Mr Assange's mental health'. See Richard Crump, 'WikiLeaks' Assange Avoids US Extradition On Suicide Fears', *Law360* (4 Jan. 2021), https://www.law360.com/articles/1341114. The US government appealed the decision and, on 27 October 2021, a two-day hearing commenced in which the US government made assurances to the High Court of England and Wales (EWCA) about Assange's treatment by the United States. At the time of writing, the parties are awaiting EWCA's decision. See Eloise Barry, 'What to Know About Julian Assange's Extradition Appeal', *Time* (29 Oct. 2021), https://time.com/6111765/julian-assange-extradition-appeal-case/; Richard Crump, 'US Wins Bid To Expand Scope Of Assange Extradition Appeal', *Law360* (11 Aug. 2021), https://www.law360.com/corporate-crime-uk/articles/1411771/us-wins-bid-to-expand-scope-of-assange-extradition-appeal.

37 This approach, however, requires careful consideration of the collateral consequences of successfully defeating extradition, including the possibility that the United States may issue a superseding indictment or bring new charges and initiate another extradition proceeding, even after their first attempt at extradition fails. In addition, the client likely will be effectively prohibited from travelling to any country with which the United States has an extradition agreement because of the risk that the United States could initiate extradition proceedings in that jurisdiction.

38 Another consideration relevant to assessing the strength of the evidence is that a client is not legally entitled to discovery from the US government related to the underlying criminal

© Law Business Research 2021

other hand, if the client has a strong case to defend against the underlying charges, he or she may wish to waive extradition, fight the charges in the United States, and attempt to assert the rule of specialty should the United States later try to supersede with additional or more serious charges.[39]

- *The client's goals*: Clients may nonetheless prefer to defer extradition for personal, family or similar reasons, even if they are unlikely to succeed in defeating it altogether. For example, if the client has health issues requiring treatment, or wants to remain close to relatives, it may be prudent to litigate extradition. Conditions of confinement may also impact the decision, for example, if the client obtains a favourable bail package in the arresting state, he or she may prefer to delay extradition to the United States, where bail conditions may be uncertain and conditions of confinement more difficult. On the other hand, if the client is confined under harsh prison conditions in the arresting state, he or she may choose to waive extradition if a bail package can be agreed to with US authorities and blessed by the court.[40]

---

charges until he or she makes an appearance in a US court. While the foreign court presiding over the extradition proceeding may have discretion to grant discovery pursuant to its 'inherent power', any discovery obtained (if at all) will be limited in scope and nature. See *Quinn v. Robinson*, 783 F.2d 776, 817 n.41 (9th Cir. 1986); see also *Oen Yin-Choy v. Robinson*, 858 F.2d 1400, 1407 (9th Cir. 1988). Accordingly, in most cases, clients will not receive any discovery until extradited (by force or consent), making it challenging to accurately assess the strength of the government's evidence. Counsel likely will have access only to evidence the client has in his or her possession, information gleaned from co-defendants (pursuant to a joint defence agreement), and evidence provided by the US government, which is likely to be scant (or non-existent) if the client is resisting extradition.

39 US courts are divided on whether an individual defendant has standing to raise a 'rule of specialty' challenge. In some circuits, the defendant has the right to raise a doctrine of specialty challenge. See, e.g., *United States v. Stokes*, 726 F.3d 880, 889 (7th Cir. 2013) (collecting cases). Other circuit courts hold, on the other hand, that rule of specialty objections can be raised only by the sending nation, not the individual defendant. See, e.g., *United States v. Suarez*, 791 F.3d 363, 366–67 (2d Cir. 2015); *United States ex rel. Saroop v. Garcia*, 109 F.3d 165, 168 (3d Cir. 1997). Some of the remaining circuits take the middle ground, allowing the defendant to raise a rule of specialty claim unless the sending nation consents to the deviation, while still others have not expressed an opinion. See *Stokes*, 726 F.3d at 889 (collecting cases). See note 45 infra.

40 For example, a review by HM Inspectorate of Prisons of HMP Wandsworth, which generally houses requested persons who are remanded in the United Kingdom pending extradition proceedings, found a number of shortcomings in the prison's management of conditions during the covid-19 pandemic. Potentially dangerous conditions include the facility's narrow Victorian-era prison landings, which render social distancing especially problematic; symptomatic prisoners locked in their cells for up to two weeks with no opportunity to shower; and non-English speaking prisoners not being provided sufficient information concerning pandemic arrangements. See HM Chief Inspector of Prisons, Report on Short Scrutiny Visits to Local Prisons (28 April 2020), https://www.justiceinspectorates.gov.uk/hmiprisons/wp-content/uploads/sites/4/2020/05/Locals-SSV-web-2020.pdf.

© Law Business Research 2021

- *Costs and resources*: Litigating extradition is expensive and resource-intensive. Clients, especially those with limited resources, may wish to direct finite resources to fighting the underlying criminal case.

These considerations must be balanced against the risk that if the United States successfully extradites the client, authorities likely will view prior resistance to extradition as avoiding responsibility or purposefully delaying the criminal case. Both could negatively impact the disposition of the case, impeding an effort to secure bail upon extradition and foreclosing or limiting favourable plea offers, co-operation opportunities, or sentencing recommendations.[41]

If a client waives extradition, the procedure typically involves filing an affidavit of consent in the responding state acknowledging that the extradition requirements have been met.[42] Individual states may have additional requirements to perfect waiver. Not all treaties allow waiver, in which case waiver may be denied.[43]

Regardless of which option a client chooses, it is critical to retain extradition counsel in the responding state. Extradition proceedings have serious implications for a client's liberty and involve multiple foreign jurisdictions. Experienced counsel is necessary to identify potential defences, attend court appearances, and communicate with foreign counterparts.

Defences to extradition 18.3.4

Defences to extradition are limited, as the responding state generally must grant extradition provided treaty requirements are met. Ultimately, the specific language of the treaty at issue and, in some cases, the laws of the responding jurisdiction,[44] determine which defences are available.[45] Common defences include the following:

- *Where the offence occurred*: Historically, many treaties did not permit extradition for crimes for which the United States asserts extraterritorial

41 This risk is particularly acute for clients who are likely to become co-operating witnesses or plead guilty, as US authorities typically view resisting extradition as non-co-operation. For this reason, it is not uncommon for US authorities to require waiver of extradition as a precondition to co-operation or before they will even consider the client as a potential co-operating witness.

42 Hedges, supra note 17, at 8–10.

43 See Bruce Zagaris, U.S. Efforts to Extradite Persons for Tax Offenses, 25 *Loy. L.A. Int'l & Comp. L. Rev.* 653, 676 (2003) (US extradition treaties that entered into force prior to 1980 do not provide for waiver of extradition); see, e.g., Extradition Treaty, Austl.–U.S., 8 May 1976, 27 U.S.T. 957; France Extradition Treaty, supra note 21, art. 3(1).

44 For instance, in the United Kingdom, local law provides several specified grounds for defending against extradition. See Extradition Act 2003, c. 41, §§ 81, 87, 13.

45 Defences that may be available to a client upon arriving in the United States for trial typically are not available at the extradition stage. For example, the foreign judge presiding over the extradition proceeding may refuse to admit evidence supporting a defence of insanity or alibi,

© Law Business Research 2021

See Chapter 17 on individuals in cross-border proceedings: the UK perspective

jurisdiction.[46] Another example of the location of the alleged misconduct operating as a defence is found in the UK's 'forum bar', which has recently been successfully invoked in multiple cases. The majority of modern treaties now require extradition regardless of where the offence occurred or allow extradition provided that the signatory countries' criminal laws are compatible.[47]

- *Nature of the offence*: The next defence is whether the offences in question are extraditable under the language of the applicable treaty. For example, in dual criminality treaties, extradition typically is denied where the alleged offence is not a crime in the responding state.[48]
- *Procedural issues*: Procedural defences may be available based on deficiencies in the extradition proceeding,[49] for example insufficiencies in the United States' filings, such as a lack of signature or failure to produce the warrant.[50] Counsel also should consider whether any statute of limitations or double jeopardy defences apply.[51]

---

which may be raised as defences to the underlying substantive offences in the US criminal proceeding. See, e.g., *Charlton v. Kelly*, 229 U.S. 447, 462 (1913) (holding that the extradition magistrate properly excluded the evidence of insanity at the hearing stage); see also *Shapiro v. Ferrandina*, 478 F.2d 894, 901 (2d Cir. 1973). These defences are likely to be available only when the client arrives in the United States. Similarly, once a client has been extradited to the United States, he or she may assert the rule of specialty, which provides that defendants may be tried by the requesting state only for the specific offences for which extradition is granted. See *United States v. Lopesierra-Gutierrez*, 708 F.3d 193, 205–06 (D.C. Cir. 2013); *United States v. Lomeli*, 596 F.3d 496, 501 (8th Cir. 2010).

46 Criminal Resource Manual, supra note 6, § 603.

47 See, e.g., Extradition Treaty, Jordan–U.S., art. 2(4), 28 March 1995, S. Treaty Doc. No. 104-3; Extradition Treaty, Austria–U.S., art. 2(6), 8 January 1998, T.I.A.S. 12916; Extradition Treaty, Lux.–U.S., art. 2(1), 1 October 1996, T.I.A.S. 12804; Extradition Treaty, Hung.–U.S., art. 2(4), 1 December 1994, T.I.A.S. 97-318; Extradition Treaty, Bah.–U.S., art. 2(4), 9 March 1990, T.I.A.S. 94-922; France Extradition Treaty, supra note 21, art. 2(4).

48 See, e.g., UK Extradition Treaty, supra note 20, art. 2(1). This defence may be particularly relevant in the FCPA context, as many countries do not outlaw certain forms of payment to government officials that are prohibited as bribery under the FCPA. For example, in 2005, the US authorities indicted a Czech national residing in The Bahamas for participating in a scheme to bribe foreign government officials. Despite the existence of a US–Bahamian extradition treaty, the Bahamian courts ruled that the defendant could not be extradited because the charges against him were for acts that, if committed in the Bahamas, would not constitute a crime. See *Superintendent of Her Majesty's Foxhill Prison & U.S. v. Kozeny,* Privy Council Appeal No. 0073, § 53 (Judicial Comm. of the Privy Council 28 March 2012) (BAH.).

49 Justice Manual, supra note 6, §§ 9-15.240, 9-15.250.

50 id. § 9-15.240.

51 These defences typically can be raised only where the applicable treaty specifically provides for such defences. See *In re Extradition of Chan Seong-I*, 346 F. Supp. 2d 1149, 1157 (D.N.M. 2004); *United States v. Neely*, 429 F. Supp. 1215, 1225 n.9 (D. Conn. 1977); Michael John Garcia and Charles Doyle, Cong. Research Serv., 98-958, Extradition to and from the United States: Overview of the Law and Recent Treaties 15–16 (2010), https://fas.org/sgp/crs/

© Law Business Research 2021

- *Humanitarian considerations*: Humanitarian defences may apply. Many states deny extradition where the requesting state may pursue the death penalty[52] or has inhumane prison conditions.[53] The latter may be a particularly acute concern for clients facing extradition in the midst of the covid-19 pandemic, which hit prisons (at least in the United States) particularly hard and may pose an especially grave threat to clients with underlying health conditions, given the wide variation in measures to address concerns about overcrowding, healthcare and hygiene at US prison facilities. Practitioners should consider whether prison conditions in the United States in the current circumstances would subject the client to inhumane treatment, especially because many US courts have been willing to grant bail to defendants who were particularly at risk of covid-19.[54] In addition, a handful of states allow individuals to assert lack of mental competency as a defence.[55] However, the US government is often successful in defeating humanitarian defences by making certain undertakings, for example agreeing that it will not seek the death penalty.[56]

---

misc/98-958.pdf (citing extradition treaties that include provisions addressing lapse of time); UK Extradition Treaty, supra note 20, arts. 2, 5, 6; *In re Ryan*, 360 F. Supp. 270, 275 (E.D.N.Y. 1973), aff'd, 478 F.2d 1397 (2d Cir. 1973).

52 See, e.g., UK Extradition Treaty, supra note 20, art. 7.

53 For instance, in May 2019, a Dutch court suspended the extradition of an individual to the United Kingdom due to 'inhuman or degrading' conditions in a British prison. See Kaya Burgess and Jonathan Ames, 'Dutch court refuses extradition to UK's "inhumane" prisons', *The Times* (11 May 2019), https://www.thetimes.co.uk/article/dutch-court-refuses-extradition-to-uk-s-inhumane-prisons-w9dvjkqpm.

54 For example, UK extradition courts have considered in recent cases whether extradition to the US should be denied due to prison conditions. In *Hafeez v. USA* [2020] EWHC 155 (Admin), the requested person argued that detention at New York City's Metropolitan Correctional Center would breach his rights under Article 3 of the European Convention on Human Rights 1950 because there was a real risk he would be kept in solitary confinement or ultimately housed at a Supermax facility, given that he faced a serious risk of being sentenced to life imprisonment without parole if convicted. The UK court determined that none of the statutory bars to extradition applied, and the Secretary of State for the Home Department ordered extradition. Following an unsuccessful appeal, Hafeez applied to the European Court of Human Rights, which instructed the UK government to consider whether in light of the covid-19 pandemic, conditions of detention in the United States would pose risk of a breach of Article 3 to Hafeez, who suffers from asthma and diabetes. See *Hafeez v. UK* (Application No. 14189/20); see also Kern and Brieskova, Prison Conditions and Extradition, supra note 34.

55 Jennifer Piel et al., 'Determining a Criminal Defendant's Competency to Proceed With an Extradition Hearing', 43 *J. Am. Acad. Psychiatry & L.* 201, 202-03 (Jun. 2015), http://jaapl.org/content/jaapl/43/2/201.full.pdf.

56 In 2001, for example, the Supreme Court of Canada ruled that it would not extradite two individuals who allegedly confessed to a brutal triple murder unless the Canadian government received assurances that the individuals would not be subject to the death penalty in the United States. Canada is entitled to seek such assurances under its extradition treaty. Extradition Treaty, Canada–U.S., art. 6, March 22, 1976, 27 U.S.T. 983.

© Law Business Research 2021

18.3.5 Appealing extradition orders

Although extradition orders typically are not appealable,[57] counsel should consult with experienced counsel in the responding state, as local law may allow for appeal.[58] Even if no appeal is made, the United States may file a new complaint to begin a separate extradition proceeding if unsuccessful in the first. Courts have uniformly held that there is no limit to how many times the United States may renew an extradition request,[59] even when based on the same evidentiary facts as the earlier request and regardless of whether it was previously denied on the merits or procedural grounds.[60] Similarly, clients may always challenge an adverse extradition ruling by petitioning for a writ of *habeas corpus* in the United States.[61] The US court's ruling on such a petition is appealable,[62] and the court may choose to stay the foreign extradition proceeding during the appeal.[63]

---

57 *Collins v. Miller*, 252 U.S. 364, 369 (1920) ('proceeding before a committing magistrate in international extradition is not subject to correction by appeal'); *In re Mackin*, 668 F.2d 122, 127–28 (2d Cir. 1981) (citing over a dozen cases holding the same).

58 In the United Kingdom, for example, extradition decisions are appealable by both the individual and the requesting state. Extradition: processes and review, Gov.UK, https://www.gov.uk/guidance/extradition-processes-and-review#extradition-from-the-uk-category-2-territories.

59 See *Collins v. Loisel*, 262 U.S. 426, 429 (1923) (holding that double jeopardy does not apply to extradition decisions).

60 Renewed requests are generally heard by a different judicial officer and reviewed *de novo*. See *Ahmad*, 910 F.2d 1063, 1065 (2d Cir. 1990); *In re Extradition of Mackin*, 668 F.2d 122, 137 n.2 0 (2d Cir. 1981); *Hooker v. Klein*, 573 F.2d 1360, 1369 (9th Cir. 1978); *In re Gonzalez*, 217 F. Supp. 717, 720 (S.D.N.Y. 1963). Subsequent extradition requests may be based exclusively on evidence submitted in the initial request or supplemental evidence. See, e.g., *Hooker*, 573 F.2d at 1366 (government's renewal of its extradition request was valid despite its first request being 'denied following an extensive evidentiary hearing and full consideration of the merits of the case by an extradition court'); *accord Mirchandani v. United States*, 836 F.2d 1223, 1226 (9th Cir. 1988); *In re Extradition of Tafoya*, 572 F. Supp. 95, 97 (W.D. Tex. 1983); cf. *Ahmad v. Wigen*, 726 F. Supp. 389, 397 (S.D.N.Y. 1989), aff'd 910 F.2d 1063 (2d Cir. 1990); see also *Ntakirutimana v. Reno*, 184 F.3d 419, 423 (5th Cir. 1999); *In re Extradition of Mackin*, 668 F.2d 122, 137 n.20 (2d Cir. 1981).

61 See 28 U.S.C. § 2241; see, e.g., *Ahmad*, 910 F.2d at 1065 ('An extraditee's sole remedy from an adverse decision is to seek a writ of *habeas corpus*; the Government's sole remedy is to file a new complaint.'). The scope of habeas review is narrower than traditional appellate review and essentially limited to three inquiries: (1) the adequacy of the trial judge's jurisdiction; (2) whether the offence is covered by the relevant treaty; and (3) whether there was sufficient evidence to support probable cause. John T Parry, 'The Lost History of International Extradition Litigation', 43 *Va. J. Int'l L.* 93, 97 (2002).

62 Criminal Resource Manual, supra note 6, § 622.

63 The writ of *habeas corpus* may be filed before an individual is extradited to the United States. However, the DOJ takes the view that '[t]he filing of the [*habeas*] petition does not automatically stay further proceedings, and in certain cases the government may go forward with the extradition if the proceedings are not stayed by the order of the [US federal] court.' Criminal Resource Manual, supra note 6, § 622.

© Law Business Research 2021

Recent developments 18.3.6

There has been significant extradition activity in the last few years. New extradition treaties took effect in 2019, including treaties between the United States and Serbia and Kosovo.[64] In addition, in December 2019, the United States signed an extradition and mutual legal assistance agreement with Croatia.[65] Furthermore, in August 2020, US government suspended its extradition treaty with Hong Kong, following international calls to halt extradition in response to China's imposition of a sweeping new national security law.[66]

In recent years, the US government also sought and successfully executed a number of extraditions, though extraditions inevitably slowed in 2020 as a result of the covid-19 pandemic.[67] In perhaps the highest-profile case of 2019, UK authorities provisionally arrested WikiLeaks founder Julian Assange to face extradition to the United States, and they remain ongoing.[68] US authorities also continue to actively seek extradition for FCPA offences[69] consistent

64 U.S. Dep't of State, 2019 Treaties and Agreements, https://www.state.gov/2019-TIAS/.

65 See DOJ, Press Release, 'United States and Croatia Sign Bilateral Agreements Enhancing Law Enforcement Cooperation', https://www.justice.gov/opa/pr/united-states-and-croatia-sign-bilateral-agreements-enhancing-law-enforcement-cooperation.

66 See BBC, Hong Kong: 'US suspends extradition treaty over national security law', BBC, https://www.bbc.com/news/world-asia-china-53844263. See Susan Zheng, 'International call to halt extradition treaties with Hong Kong after China imposes tough national security law', *SCMP* (6 July 2020), https://www.scmp.com/news/china/diplomacy/article/3091960/international-call-halt-extradition-treaties-hong-kong-after.

67 Among others, the United States was successful in extraditing an individual from Serbia in February 2021 in connection with an alleged US$70 million fraud targeting investors in binary options and cryptocurrency mining. See DOJ, Press Release, 'Serbian Man Extradited to U.S., Charged with $70 Million Fraud in North Texas' (5 Feb. 2021), https://www.justice.gov/usao-ndtx/pr/serbian-man-extradited-us-charged-70-million-fraud-north-texas. In addition, in April 2021, the United States successfully extradited a Nigerian citizen and resident of Canada from Germany to face charges for his alleged involvement in a 'spoofing' service used to steal millions of dollars from individuals' and corporations' bank accounts. See DOJ, Press Release, 'U.S. Attorney Announces Extradition Of Canadian Citizen For His Role In An International Fraud And Money Laundering Network' (9 Apr. 2021).

68 See supra, note 36.

69 For example, in May 2019, a Malaysian national previously arrested in Malaysia waived extradition and made his first appearance in US federal court to face charges for conspiring to engage in a multibillion-dollar money laundering scheme and violate the FCPA by bribing foreign public officials to embezzle billions of dollars from 1MDB, Malaysia's sovereign wealth fund. See DOJ, Press Release, 'Former Banker Extradited from Malaysia to United States to Face Charges in Multi-Billion Dollar Money Laundering and Bribery Scheme Relating to the 1MDB Fund' (6 May 2019), https://www.justice.gov/opa/pr/former-banker-extradited-malaysia-united-states-face-charges-multi-billion-dollar-money. Notably, Malaysian authorities have described the defendant's extradition to the United States as a 'temporary surrender' so that they may later pursue charges for similar conduct brought against him in Malaysia. See Matthew Goldstein, 'Former Goldman Sachs Banker Pleads Not Guilty in

© Law Business Research 2021

with the DOJ's and SEC's increasingly broad view of their mandate to enforce the FCPA.[70]

18.4 Strategic considerations

There are a number of strategic considerations counsel must bear in mind in advising a white-collar client navigating a criminal, civil or internal investigation or proceeding. While certain of these considerations are common to all three contexts, others are particular to criminal actions or internal investigations.

18.4.1 Assessing the client's status

In all three contexts – criminal, civil and internal – counsel must first assess a client's status with respect to a current or potential criminal action (should one later be initiated). Individuals who come into the orbit of a US criminal investigation fall into one of three categories: witness, subject or target.[71] Counsel must assess the client's status to advise on strategic options, which will vary depending on status. For this reason, it is common for counsel to seek clarification from the DOJ regarding a client's status. However, even if a client is a witness, the designation may change as the investigation progresses. It is therefore critical to independently and continuously assess the client's exposure to advise on the relevant risks and strategic options.

Malaysia Fraud Case', *N. Y. Times* (6 May 2019) at B3, https://www.nytimes.com/2019/05/06/business/goldman-sachs-roger-ng-1mdb.html. At the time of writing, his case is still pending in the United States, with the long-delayed trial scheduled to proceed on 18 January 2022. See Stewart Bishop, 'Judge Rejects Ex-Goldman Exec's Bid To Avoid 1MDB Trial', *Law360* (10 Sep. 2021), https://www.law360.com/articles/1420785/judge-rejects-ex-goldman-exec-s-bid-to-avoid-1mdb-trial.

70 See generally DOJ and U.S. Sec. Exch. Comm'n, A Resource Guide to the U.S. Foreign Corrupt Practices Act Second Edition (Jul. 2020); see also 'Should FCPA "Territorial" Jurisdiction Reach Extraterritorial Proportions?', Am. Bar Ass'n, (8 Nov. 2018), https://www.americanbar.org/groups/international_law/publications/international_law_news/2013/should_fcpa_territorial_jurisdiction_reach_extraterritorial_proportions/.

71 Under federal law, a 'witness' is someone who authorities believe has information about facts relevant to a criminal investigation and who assists prosecutors in obtaining indictments against other individual or companies. A 'subject', by contrast, is 'a person whose conduct is within the scope of the grand jury's investigation', i.e., someone who engaged in activity or conduct at issue in the prosecutor's investigation, but who the prosecutor has not yet determined participated in criminal activity. A 'target' is 'a person as to whom the prosecutor or the grand jury has substantial evidence linking him to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant'. Justice Manual, supra note 6, § 9-11.151.

© Law Business Research 2021

Decision to co-operate 18.4.2

Co-operating with or defending a criminal or civil proceeding 18.4.2.1

A client facing criminal or civil prosecution must choose whether to co-operate with authorities or fight the case.[72] Co-operation may be an attractive option to reduce the potential sentence or financial penalties. But these potential benefits are not without risks. The client must understand the duties that accompany co-operation, including admitting criminal conduct, meeting with the government to provide information about his or her (and others') involvement, and potentially testifying against others at trial. The client also must disclose any other potential misconduct, even if outside the scope of the investigation, and be fully transparent about his or her finances. In determining whether to recommend co-operation, counsel should assess the quality of the client's information, its likely usefulness to the government's case, and the client's capacity for candour and ability to endure probing proffer sessions or trial.

Co-operation typically begins with attorney proffers, during which counsel 'previews' for the government the information that the client can provide.[73] The client will then typically meet with the government for multiple proffer sessions before entering into a formal co-operation agreement to resolve the charges. Client proffers should typically be conducted only after negotiating a proffer agreement, which provides limited protections from the government's future use of any statements made. In addition, before the proffer, counsel should advise the client that he or she cannot be forced to provide information to the government, discuss the consequences of voluntarily speaking with the authorities, and ensure that the client understands the limited protections and potential pitfalls of any proffer agreement.[74]

---

72 The government often relies on co-operating witnesses in white-collar cases, both during the investigatory phase and also at trial, e.g., to explain otherwise complicated and document heavy cases. See, e.g., *Kastigar v. United States*, 406 U.S. 441, 446 (1972) ('[M]any offenses are of such a character that the only persons capable of giving useful testimony are those implicated in the crime.') Individual co-operators tend to be lower-level employees or those who are less culpable in the criminal conduct. In particularly complex white-collar cases, the government may rely on more culpable individuals to co-operate against the primary target of an investigation or a company involved in a criminal scheme.

73 During the attorney proffer, counsel should explain to the government counsel's understanding of how the client was involved in the conduct under investigation and outline the information the client will be able to provide to the government. The attorney proffer is a critical opportunity to assess how the government is likely to react to the client's testimony, identify potential risk areas, and potentially learn more about the government's evidence and theory of the case depending upon the prosecutors' questions and reactions.

74 The proffer agreement typically includes a provision that the government will not use statements made during the interview directly against the client. See *United States v. Rosemond*, 841 F.3d 95, 109–10 (2d Cir. 2016). However, the government may use the statements for other purposes, e.g., as a lead to obtain other evidence or, if the client

© Law Business Research 2021

Clients co-operate with the hope, but no guarantee, of receiving a recommendation from the government for a reduced sentence. Practically speaking, this is delivered in a '5K1.1 letter' from the government recommending a lower sentence than would otherwise be imposed in exchange for co-operation (or 'substantial assistance').[75] Alternatively, clients may receive a deferred prosecution agreement (DPA), under which all charges are dropped after certain conditions are met.[76] A DPA is preferable to a 5K1.1 letter but is harder to obtain.

Many clients choose to co-operate after they have been indicted. In these circumstances, clients usually must decide relatively quickly whether to co-operate, as timeliness of co-operation and acceptance of responsibility will impact the government's plea offer, sentencing recommendation and, ultimately, the court's sentence.[77] Clients may have the opportunity to co-operate pre-indictment, though this typically requires that counsel be involved and proactively engage with the government from the investigation's outset. In these situations, clients may be able to resolve the proceedings through a non-prosecution agreement (NPA), in which authorities decline to bring any charges.[78]

Co-operation is not the right path for all clients. Several legal and personal factors may lead the client to fight the case. In those cases, counsel must carefully

later testifies at trial in his own defence, the government can usually offer into evidence contradictory statements made during proffer sessions.

75 § 5K1.1 of the US Sentencing Guidelines enables the government to make a motion to allow the court to sentence a defendant below the applicable Sentencing Guidelines range. See Federal Sentencing Guidelines Manual § 5K1.1. In such motions, the government typically will set forth the nature, usefulness and significance of the client's assistance during the proffer process. To receive credit for substantial assistance, the client will at a minimum need to be fully transparent about his own illicit conduct and to provide information about other people involved in the criminal activity. The client may also be required to produce documents, participate in investigatory operations (e.g., wearing a wire to record conversations with other defendants or targets), or testify before a grand jury or at trial. Importantly, a 5K1.1 letter is no guarantee of a favourable or reduced sentence, as the court retains discretion to impose a sentence up to the statutory maximum. See Federal Sentencing Guidelines Manual § 5K1.1 (2018) (explaining that a court '*may* depart from the guidelines' in the case of a defendant's substantial assistance to authorities) (emphasis added).

76 A DPA sets out certain conditions that must be met before charges in the indictment will be dropped. Such conditions typically include a fine, term of supervision by pretrial services, or community service. DPAs are typically available only after the client has provided substantial co-operation, including potentially acting as an informant. See, e.g., Enforcement of the FCPA – Criminal Procedures – Deferred Prosecution Agreements, 13 Bus. & Com. Litig. Fed. Cts. § 134:34 (4th ed.).

77 See Federal Sentencing Guidelines Manual § 5K1.1(5).

78 To obtain an NPA, the client usually must pay a fine and co-operate with the government. In exchange, the relevant agency will refrain from filing criminal or civil charges. In deciding whether to enter into an NPA, DOJ policy provides that prosecutors should balance the cost of forgoing prosecution with the need for the co-operation to the public interest. Justice Manual, supra note 6, § 9-27.600 (2018).

© Law Business Research 2021

research and evaluate the client's likelihood of criminal liability and potential defences, including limitation periods and jurisdiction. It is also important to understand the client's personal, financial and family circumstances. Some clients who have a reasonable likelihood of successfully defending the case may nevertheless choose to co-operate because of the collateral consequences of a criminal trial.

Co-operating with an internal investigation 18.4.2.2

In advising a client on co-operating with an internal investigation, counsel should first assess whether the client is a current employee with a duty to co-operate under relevant laws, employment agreements or company policies.[79] If a client is a former employee, he or she nonetheless may be required to co-operate under the terms of any deferred compensation or separation package.[80] Counsel should advise all clients to consider the ramifications of not co-operating on employment prospects and their relationship with the company.

Counsel must also assess whether co-operation will jeopardise Fifth Amendment protections. While private employees generally do not have a Fifth Amendment right against self-incrimination in internal investigations, the right applies where co-operation is compelled (e.g., threat of termination or economic consequence such as unpaid suspension), and the employer's actions are 'fairly attributable' to the government.[81] For example, a US federal district court recently held that an employee's statements were 'compelled testimony' protected by the Fifth Amendment in an internal investigation conducted by his employer at the direction of an enforcement agency.[82] Accordingly, while a client cannot assert the Fifth Amendment in a purely internal investigation, he or she can likely do so where the investigation is conducted at the government's behest, the government has substantial input into the investigation or the government has effectively 'outsourced' its investigation to the employer or its counsel.[83]

See Chapters 10 on co-operating with authorities and 14 on employee rights

79 It is now commonplace for employers to write into employment agreements and internal policies a requirement that employees co-operate in internal investigations. Failure to do so can be grounds for disciplinary action, including suspension without pay or termination. It may be necessary to engage employment counsel to advise the client on co-operation obligations under relevant employment agreements, policies or labour law in the relevant jurisdiction.

80 Clients should be made aware that, even where no formal or legally enforceable co-operation obligation exists, employers may withhold deferred compensation or post-employment remuneration to incentivise co-operation with an internal investigation.

81 *Garrity v. New Jersey*, 385 U.S. 493, 497 (1967); see also *United States v. Connolly*, No. 16 CR. 0370 (CM), 2019 WL 2120523, at *10 (S.D.N.Y. 2 May 2019).

82 *Connolly*, 2019 WL 2120523, at *14.

83 See id. at *11–14. On the other hand, if the company acted entirely on its own, the resulting statements are not 'compelled' by state actors within the meaning of the Fifth Amendment and are therefore freely usable by the government at any later point in time.

© Law Business Research 2021

Finally, counsel must consider the criminal, civil or regulatory consequences of co-operation, including the possibility that the company will share the substance of the client's interview with criminal or civil enforcement authorities.[84] While the client's communications during such interviews are typically privileged in the United States, the underlying facts are not. Further, the privilege belongs to the employer,[85] and the employer may choose to waive privilege, including through self-reporting or compelled disclosure.[86] By the same token, counsel should consider the consequences of not co-operating, particularly in jurisdictions such as the United Kingdom, where persons approved by the Financial Conduct Authority have a positive obligation to co-operate and failure to do so could jeopardise licensed status.[87]

See Chapter 8 on witness interviews

18.4.3 Dealing with multiple authorities

18.4.3.1 Voluntary interviews

An additional consideration that often arises in cross-border proceedings is how evidence collected and statements made in one jurisdiction can be used by authorities in another. This issue is increasingly important because the United States is more frequently coordinating white-collar investigations with foreign authorities. It has also become common for foreign authorities to conduct parallel investigations into the same or related conduct, regardless of whether there is express coordination with US authorities.[88]

Counsel must consider what impact investigations and corresponding procedures in other jurisdictions may have on US proceedings. One key consideration in this respect is whether a client might waive Fifth Amendment rights by testifying in a foreign proceeding, opening the door for that testimony to be used against the client in a present or future criminal or civil proceeding against the client in the United States.[89] Providing some comfort to clients who are

84 For example, counsel should carefully assess whether co-operation will increase the risk that a parallel criminal action is brought against the client by US prosecutors or by civil authorities in a foreign jurisdiction in which the client is licensed or regulated.

85 Company counsel likely will inform the client accordingly in an *Upjohn* warning at the beginning of any interview. See *Upjohn*, 449 U.S. 383, 394 (1981); Model Rules of Prof'l Conduct r. 1.13(f), 4.3. Counsel should similarly advise clients, particularly where they may provide information that could be used against them in a future enforcement proceeding.

86 The company may even decide to turn over the notes or summaries of the interview, or may be required to do so under the laws of the relevant jurisdiction.

87 See *Statement of Principle and Code of Practice for Approved Persons*, UK Financial Conduct Authority (FCA), § 2.1A.3 (September 2019), https://www.handbook.fca.org.uk/handbook/APER.pdf (Statement of Principle 4 provides that '[a]n *approved person* must deal with the *FCA*, the *PRA* and other regulators in an open and cooperative way and must disclose appropriately any information of which the *FCA* or the *PRA* would reasonably expect notice') (emphasis in original).

88 See, e.g., infra note 90.

89 U.S. Const. amend. V; see *United States v. Saechao*, 418 F.3d 1073 (9th Cir. 2005).

© Law Business Research 2021

compelled to provide testimony in foreign proceedings, at least one US court has held that the Fifth Amendment's prohibition on the use of compelled testimony extends to testimony compelled by a foreign authority, 'even when the testimony was compelled . . . in full accordance with [foreign] law'.[90]

Counsel should also consider whether a client's voluntary interview with a foreign authority would require discussion of subject matter otherwise protected by the attorney–client privilege and therefore waive privilege, permitting US authorities to use that information in their own proceedings. In these situations, it is often advisable to consult with local counsel to confirm the client's obligations and potential risks of refusing the interview request in the foreign jurisdiction.

Evidence obtained pursuant to mutual legal assistance treaty 18.4.3.2

If a client does not co-operate, US authorities may seek testimonial or documentary evidence via mutual legal assistance treaty (MLAT) request.[91] The MLAT process can be slow, taking more than a year between the time a request is made and the time testimony is taken or documents produced.[92] Although most MLATs permit the requesting authority to be present during questioning, the interviews are typically conducted by foreign law enforcement officials pursuant to local procedural rules. This means that certain protections available in the United States may not apply, for example the right to counsel

90 *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017) (reversing convictions of two Rabobank traders who provided testimony to the FCA in an investigation into LIBOR manipulation under threat of prosecution for non-co-operation under UK law, because the Fifth Amendment 'prohibits the use and derivative use of such compelled testimony in an American criminal case against the defendant who provided that testimony').

91 The United States has entered into MLATs or similar bilateral agreements with approximately 70 states allowing it to enlist the investigatory authority of those states to procure evidence. See generally, Treaties in Force 2020 and Treaties in Force 2021 Supplement, supra note 22. In addition, the United States is party to an agreement with the European Union that enhances mutual legal assistance mechanisms with EU Member States. See Mutual Legal Assistance Treaty, European Union–U.S., 16 January 1998, T.I.A.S. 12923. The DOJ's Office of International Affairs (with the Department of State) negotiates and implements MLATs, administers mutual legal assistance operations, and coordinates incoming and outgoing requests. Notably, unlike extradition treaties, MLATs generally do not require dual criminality.

92 See United Nations, Manual on Mutual Legal Assistance and Extradition (Sep. 2012), https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf. For this reason, a request for mutual legal assistance to a foreign authority is often accompanied by a petition to a US court under 18 U.S.C. § 3292 to suspend the running of the statute of limitations during the pendency of a request. A court will grant the request if it finds by a preponderance of the evidence that an official request has been made and it reasonably appears that the evidence is or was in a foreign country. See, e.g., T Markus Funk, Federal Judicial Center International Litigation Guide: Mutual Legal Assistance and Letters Rogatory: A Guide for Judges 15 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf.

© Law Business Research 2021

or attorney–client privilege. Accordingly, local counsel is essential to navigating the interview process in the foreign jurisdiction.

18.4.4 Counsel selection

A client must also select counsel, which entails deciding whether to engage independent counsel or pursue joint or pool counsel representation with counsel for an employer or colleagues, or both.

Where the representation relates to a client's current or former employment, many employers encourage retaining company counsel, particularly when the client is a current employee. For purely internal investigations, or where there is no indication of individual wrongdoing, an employee may not feel the need for counsel or may be happy working with company counsel. While joint representation by company counsel is often the most expedient and economical choice for employers, company counsel is not always the right choice for the individual client and ultimately may be problematic for the company. The opportunity for conflicts to arise in a joint representation is substantial, particularly where the client may give testimony contradicting the employer's position or creating liability for the employer.[93] For former employees, the risk of conflict is even more acute, as employee–employer interests are even less likely to be aligned. If clients elect not to co-operate, they will have no choice but to appoint independent counsel, owing to the inherent conflict created.[94]

A client may alternatively choose to appoint pool counsel, wherein the client is represented along with several other clients by one counsel. Pool counsel is an efficient way to provide representation for multiple employees while saving time and resources. It is typically appropriate when the clients are fact witnesses with minimal or no personal exposure, or fall into the same category (e.g., former employees); the subject of the interviews is likely to be similar; or the investigation is expected to be finite. Pool counsel is not appropriate when clients may contradict or give testimony creating liability for one another. Pool counsel must vigilantly monitor for conflicts and ensure that each client is aware of the duty owed to the others. To this end, clients should be counselled about the potential conflicts and privilege implications[95] of pool

93 See also Model Rules of Professional Conduct r. 1.13 cmt. (Am. Bar Ass'n 2018) (providing that investigating counsel should advise employees whose interests may be adverse to the corporation that he or she 'may wish to obtain independent representation').

94 Counsel should also bear in mind that US authorities may take a dim view of joint representation, questioning the independence of the client's testimony or, at the most extreme, alleging that a conflict has arisen and insisting that independent counsel be retained.

95 While '[a]n employee's cooperation in an internal investigation alone is not sufficient to establish a common interest', the privilege will be deemed waived where there is 'some form of joint strategy' among the parties. *In re Grand Jury Subpoena: Under Seal*, 415 F.3d 333, 341 (4th Cir. 2005) (quoting *United States v. Weissman*, 195 F.3d 96, 100 (2d Cir.1999)); see also *United States v. Aramony*, 88 F.3d 1369, 1392 (4th Cir. 1996) ('To be entitled to the protection of this privilege the parties must first share a common interest about a legal matter.').

© Law Business Research 2021

counsel, and engagement letters should require clients' informed consent to the arrangement.[96]

See Chapter 16 on representing individuals in interviews

Regardless of the type of counsel selected, clients should also consider whether to engage specialised counsel, such as employment counsel to advise on co-operation obligations under applicable labour law or employment agreements, or counsel specialising in the law of the foreign jurisdiction, for example in jurisdictions with stringent privacy laws or circumscribed attorney–client privilege protections.

Impact of company settlement 18.4.5

Counsel must consider the impact of a company's settlement or plea agreement, which may name individual employees, reference employee conduct or admit facts implicating individual employees. The risk that a company names individual employees is particularly acute given the DOJ's policy requiring companies to report misconduct by individual wrongdoers to receive co-operation credit. Counsel should advise clients that a company's settlement or plea agreement with enforcement authorities does not necessarily extinguish potential criminal liability for the client, nor does it eliminate the potential for claims in separate civil litigation, including those, for example, in a shareholder derivative suit.

See Chapters 10 on co-operating with authorities, 24 on negotiating global settlements and 35 on parallel civil litigation

Evidentiary issues 18.5

Privilege laws across jurisdictions 18.5.1

A key consideration in cross-border proceedings is whether legal communications will be protected from disclosure to regulators and other parties. While in

Furthermore, it has become increasingly common for companies to include in joint defence agreements language that expressly allows the company to unilaterally disclose joint defence materials and information to other parties to the representation. See Ed Magarian and Surya Saxena, 'Joint Defense Agreements: What Is A Responsible Company To Do?', 22 Andrews Corp. Officers and Directors Liability Litig. Rep., September 2008, at 1 (2008).

96 In both pool and company counsel representations, counsel will need to obtain the client's consent to disclose confidential information to others in the pool and 'use' such information for the benefit of other clients (while maintaining the privilege to outside parties) under the joint defence privilege. Engagement letters also should clearly explain that pool counsel may use information provided by one client to zealously represent all clients in the pool (though information identified by a client as being confidential will only be shared with express authorisation). Relatedly, clients should be advised not to speak with any third parties about the substance of the investigation to preserve the integrity of the respective clients' recollections, and also because those communications will not be protected by the common interest or joint defence privilege. See, e.g., *United States v. Austin*, 416 F.3d 1016, 1021 (9th Cir. 2005) (joint defence privilege protects the confidentiality of communications 'passing from a party to his or her attorney' and 'from one party to the attorney for another party', but only 'where a joint defense effort or strategy' exists) (quoting *United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989)).

© Law Business Research 2021

the United States these communications are protected by the attorney–client and work-product privileges, analogous protections are not always available in foreign jurisdictions.[97]

For example, privilege protections may diverge among jurisdictions with respect to communications with in-house counsel, an issue that typically arises in internal investigations. Under US federal law and the laws of each state, the attorney–client privilege applies equally to communications with external and in-house counsel.[98] In many European countries, however, the equivalent privilege applies only to written communications between clients and external counsel.[99]

Additionally, in certain circumstances, US counsel's own communications with a foreign client may not be protected under US law. To determine whether such communications are privileged, US courts apply the 'touch base analysis', deferring to the privilege laws of the country with the 'predominant' or 'most direct and compelling interest'.[100]

Foreign privilege rules have a meaningful impact on the scope of materials and information available to investigating authorities and even counsel. It is therefore prudent to consult with local counsel to understand the scope of protections in the relevant jurisdiction.

---

97 In China, for example, there is no doctrine of legal privilege. Richard Bartlett and Yuan Min, A Lawyer's guide to working in China, King & Wood Mallesons (15 Nov. 2017), https://www.kwm.com/en/knowledge/insights/a-lawyers-guide-to-working-in-china-20171113. And while the European Union provides for the 'legal professional privilege', it is comparatively limited, covering only counsel who are admitted to the bar in one of the Members States of the European Union. Patrick Doris and Steve Melrose, Privilege: European Union, Global Investigations Review. (12 October 2018), https://globalinvestigationsreview.com/preview_jurisdiction/1005270/european%20union?preview=1000391.

98 See, e.g., *Swidler & Berlin v. United States*, 524 U.S. 399, 408 (1998); see also Doug Gallagher, Manasi Raveendran, Attorney–Client Privilege for in-House Counsel, Am. Bar Ass'n (2017), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/november-december/attorney-client-privilege-inhouse-counsel/. Privilege issues arise more often in the context of communications with in-house rather than external counsel because, for example, in-house counsel may often play the dual role of offering both legal and business advice.

99 Ava Borrasso, 'Privilege and International Implications against the Backdrop of the Panama Papers', Am. Bar Ass'n (20 July 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/07/12_borrasso/.

100 *Cadence Pharm., Inc. v. Fresenius Kabi USA, LLC*, 996 F. Supp. 2d 1015, 1019 (S.D. Cal. 2014). The country with the 'predominant interest' is either 'the place where the allegedly privileged relationship was entered into' or 'the place in which the relationship was centered at the time the communication was sent'. Id.

© Law Business Research 2021

Foreign restrictions on information transfer 18.5.2

Many countries have data protection laws restricting extraterritorial transfer of personal and corporate information. For example, the EU's General Data Protection Regulation (GDPR), which came into force in 2018, effected significant changes in data privacy.[101] The data protection and transfer laws of some countries further restrict how data can be shared or used.[102] Recently, a July 2020 ruling from the European Court of Justice invalidating a widely used EU–US data transfer agreement – the 2016 Privacy Shield agreement – may give rise to data transfer restrictions for thousands of companies, which, in turn, may affect the ability of US counsel to access such materials on behalf of their individual clients in a cross-border representation.[103]

The practical effect of such restrictions is that counsel may not be able to transfer data to the United States and will need to review relevant material in a foreign jurisdiction.[104] Similarly, there may be restrictions on the materials or information a client can disclose to US authorities in interviews or productions. Nonetheless, beginning in 2020, the United States has entered into certain data transfer agreements with certain EU countries (including the United Kingdom) to allow for transfer of data in accordance with applicable

101 The GDPR imposes certain obligations on individuals, organisations and companies who are 'controllers' or 'processors' of personal data and restricts how they may process and transfer that data. If the controller or processor wishes to transfer the data to a country the European Commission has not deemed adequate, such as the United States, it must identify whether a sufficient basis, or 'derogation', applies under the GDPR and implement safeguards to ensure GDPR compliance. One such derogation applies when the transfer is necessary for the establishment, exercise or defence of legal claims, which commonly applies in the context of criminal or other regulatory investigations, where transfer of data is necessary for the purpose of defending the individual client. See European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 11 (25 May 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

102 See, e.g., Schweizerisches Strafgesetzbuch (Swiss Criminal Code), 21 December 1937, art. 349.

103 The US Commerce Department is working to put in place a new deal with the European Union, and the Biden administration is reportedly considering taking executive action in light of the ongoing dilemma. See Sam Schechner and Valentina Pop, 'EU's Top Court Restricts Personal-Data Transfers to U.S., Citing Surveillance Concerns', *Wall Street Journal* (16 Jul. 2020), https://www.wsj.com/articles/eus-top-court-restricts-personal-data-transfers-to-u-s-citing-surveillance-concerns-11594888385?mg=prod/com-wsj; David Uberti, 'EU-U.S. Data Privacy Talks Enter Second Year With No Timeline for Resolution', *Wall Street Journal* (21 Jul. 2021), https://www.wsj.com/articles/eu-u-s-data-privacy-talks-enter-second-year-with-no-timeline-for-resolution-11626859800.

104 See, e.g., France's Law 80-538 of 16 July 1980 Relating to the Communication of Economic, Commercial or Technical Documents or Information to Foreign Natural or Legal Persons, Journal Officiel de la République Française, 17 July 1980, art. 1A (Fr.).

© Law Business Research 2021

regulations.[105] Accordingly, because relevant laws are evolving, and clients (and counsel) could expose themselves to sanctions for failing to comply with these regimes,[106] clients should consult local counsel to ensure compliance.

See Chapter 40 on data protection

18.5.3 Evidentiary considerations in internal investigations

In internal investigations, clients may be asked to provide documents, emails or other records to company counsel. Clients typically must comply if the materials were created or maintained in the course of employment, as they are considered the employer's property.[107] Failure to comply risks disciplinary action, termination or being reported to authorities as unco-operative or obstructionist.[108] For this reason, too, clients should be counselled to carefully abide by any legal holds. Even if a hold has not issued, clients should preserve all potentially relevant materials to avoid even the appearance of potential spoliation.[109]

Notwithstanding the above, former employees may be able to assert the Fifth Amendment in refusing to produce incriminating documents to US

105 For example, on 8 July 2020, the United States' and United Kingdom's historic CLOUD Act Agreement came into effect – the first such agreement of its kind. Under the agreement, law enforcement in the United States and United Kingdom may access data from communications providers located in the other jurisdiction without the need for review or pre-approval from domestic authorities. US Attorney General William Barr described the agreement as a pivotal step in enhancing the law enforcement abilities of each country, 'by allowing more efficient and effective access to data needed for quick-moving investigations.' DOJ, Letter from Assistant Att'y Gen. Stephen E. Boyd to Congress, 16 January 2020.

106 See, e.g., Swiss Criminal Code 21 December 1937, SR 757 (1938), as amended by Gesetz, 4 October 1991, AS 2465 (1992).

107 The law is not entirely settled on this issue. The critical inquiry is whether (1) the materials were created or maintained in the course of employment, and (2) the employee had a reasonable expectation of privacy with respect to the materials. See, e.g., *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (no reasonable expectation of privacy in email communications made voluntarily over company email system even where employer told employees electronic communications would be kept confidential); but see *Levanthal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (public employee had reasonable expectation of privacy in contents of office computer because, *inter alia*, employee occupied private office with closed door and had exclusive use of desk, filing cabinet and computer); *Kellher v. City of Reading*, No. CIV.A.01-3386, 2002 WL 1067442, at *1 (E.D. Pa. 29 May 2002) (acknowledging that employee may have reasonable expectation of privacy in certain company email communications depending on the communication at issue and configuration of the relevant email system).

108 Note, however, that the client may have a cognisable claim that the materials are protected by the attorney–client or other applicable privilege. See, e.g., *Sims v. Lakeside School*, No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. 20 Sep. 2007).

109 Even where a company has not requested materials, it is prudent to advise clients to preserve any emails, notes or other documents that they believe may bear on the investigation. To assure adequate preservation, it may be necessary to engage a reputable third-party forensic technician to image or otherwise preserve the documents or data in question.

© Law Business Research 2021

authorities.[110] Current employees generally do not have this right.[111] Before turning over any documents to company counsel that may be shared with authorities, counsel should seek advice from local counsel regarding the client's (and counsel's) exposure for doing so under applicable data privacy or other local laws.

Finally, in most internal investigations, individual counsel is dependent on company counsel to obtain relevant materials. To this end, a cordial and co-operative relationship with company counsel is critical to facilitate information sharing.

See Chapter 16 on representing individuals

Asset freezing, seizure and forfeiture 18.6

Counsel should advise clients regarding the potential for asset freezing, seizure or forfeiture. In criminal proceedings, the DOJ may pursue criminal or civil forfeiture of tainted assets, that is, property derived from the criminal conduct, or substitute assets up to an equivalent value, if tracing the directly forfeitable property is impossible or the tainted assets are no longer available.[112] Criminal forfeiture charges must be included in the indictment or criminal information.[113] A criminal forfeiture order typically cannot be obtained unless the client is criminally convicted of, or has pleaded guilty to, a forfeiture offence.[114] In civil proceedings, the DOJ must file an *in rem* action, namely one against the property derived from or used to perpetrate the crime,[115] and usually seizes

110 Former employees may claim an act of production privilege in refusing to produce documents 'where the act of production is, itself, (1) compelled, (2) testimonial and (3) incriminating.' *In re Three Grand Jury Subpoenas Duces Tecum Dated Jan. 29, 1999*, 191 F.3d 173, 178 (2d Cir. 1999). It is not clear, however, how a court might rule where the documents in the former employee's possession are deemed to be the company's property, e.g., where the employee took the documents upon leaving the employer without permission and/or in violation of company policy. But see id. at 182–83.

111 In *Braswell v. United* States, 487 U.S. 99, 102 (1988), the Supreme Court held that current employees may not claim the act of production privilege, even if those documents are incriminating against the employee, because the employee is an agent of the company and the records were in the employee's custody in his capacity as an agent. The Court did not address whether the outcome might differ if the records in question were personal to the employee or not maintained in his capacity as an agent of the company. In light of *Connolly*, former employees in an internal investigation conducted at the behest of the government might have an argument that the act of production privilege applies to them as well.

112 See, e.g., 18 U.S.C. §§ 981, 982; 21 U.S.C. § 853.

113 See Fed. R. Crim. P. 32.2(a).

114 See 18 U.S.C. §§ 982(a), 1963(e); Fed. R. Crim. P. 32.2(b)(1)(A). Criminal forfeiture is often included as part of a defendant's sentence. Following a finding of guilt, the government must prove its forfeiture case by a preponderance of the evidence. The sentence, including any forfeiture order, may be appealed to a higher court.

115 See 18 U.S.C. §§ 983(a)(4), 984(a)(1), 985(c); see also 18 U.S.C. § 983(a)(1); 19 U.S.C. § 1607. In contrast to a criminal forfeiture, civil forfeiture does not require a criminal conviction. Rather, property is forfeitable as an instrumentality of a criminal offence. See *United States*

© Law Business Research 2021

the property (with the exception of real property) before the court's entry of a civil forfeiture order.[116]

The DOJ also may obtain a pre-indictment or pretrial restraining order to freeze assets that have not yet been seized.[117] The SEC may similarly freeze assets through a temporary pretrial restraining order to ensure that funds for a future disgorgement order are available.[118]

If the assets subject to forfeiture are unavailable as a result of the client's act or omission, US authorities can satisfy the forfeiture order through substitute assets (other assets of the client of comparable value).[119] Counsel should discuss with clients the impact this may have on joint assets such as a home or other property shared with a spouse.[120]

US authorities have increasingly sought to freeze and seize assets in white-collar cases involving securities fraud, bribery, money laundering and insider trading, even when the assets in question are located outside the United States:[121] 2021 was no exception to that trend.[122] In addition, the DOJ continues to use its asset forfeiture powers to tackle alleged covid-19-related fraud.[123]

See Chapter 31 on individual penalties

---

v. Bajakajian, 524 U.S. 321 (1998); but see *United States v. Oriho,* No. 19-10291, 2020 WL 4579478 (9th Cir. 10 Aug. 2020).

116 Id. § 985(b)(1).

117 Id. § 983(j). The government must have probable cause to believe the property constitutes proceeds of crime or was used during the commission of a crime. See 21 U.S.C. 853(e)(2). An indictment returned by a proper grand jury 'conclusively determines the existence of probable cause'. *Kaley v. United States*, 571 U.S. 320, 328 (2014) (citing *Gerstein v. Pugh*, 420 U.S. 103, 117 n.19 (1975)).

118 *SEC v. One or More Unknown Traders in the Securities of Onyx Pharmaceuticals, Inc.*, 296 F.R.D. 241, 254 (S.D.N.Y. 2013) (citing *SEC v. Unifund SAL*, 910 F.2d 1028, 1041 (2d Cir. 1990)).

119 21 U.S.C. § 853(p).

120 See, e.g., *United States v. Butler*, 543 F. App'x 95, 97 (2d Cir. 2013).

121 The United States is a party to a number of treaties, as well as other formal and informal agreements, that provide for freezing or seizure of assets in foreign jurisdictions. See, e.g., U.S. Internal Revenue Service, Internal Revenue Manual § 9.7.10.1.2 (28 Jul. 2003), https://www.irs.gov/irm/part9/irm_09-007-010#idm140235861363504. In addition, US authorities (and private civil litigants) may register seizure or forfeiture orders issued by US courts in foreign jurisdictions in hopes of enforcing those judgments abroad. See, e.g., Mutual Legal Assistance Treaty, U.S.–U.K., art. 19(2) 6 January 1994, T.I.A.S. No. 96-1202.

122 For example, in 2021, the United States settled a civil forfeiture action against assets of Sefira Capital LLC and its subsidiaries, which allegedly accepted millions of dollars of narcotics proceeds laundered through the shadow financial system known as the Black Market Peso Exchange, for investment in various real estate ventures. See DOJ, Press Release, 'Acting Manhattan U.S. Attorney Announces Settlement Of Civil Forfeiture Claims Against Over $50 Million Laundered Through Black Market Peso Exchange' (12 Jan. 2021), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-settlement-civil-forfeiture-claims-against-over.

123 See, e.g., DOJ, Press Release, 'United States Recovers $8.4 Million In Fraudulent COVID Relief Funds From Family' (29 Apr. 2021), https://www.justice.gov/usao-mdfl/pr/united-states-recovers-84-million-fraudulent-covid-relief-funds-family; DOJ, Press Release, 'U.S. Files

© Law Business Research 2021

Collateral consequences 18.7

Counsel must be attuned to numerous collateral consequences of a cross-border proceeding. These include the potential for:

- parallel actions by other authorities (domestic or foreign);
- follow-on civil litigation by shareholders or victims;
- revocation or suspension of regulatory or professional licences or registrations;
- difficulty obtaining requisite background or 'know your customer' clearance for employment or personal finances;
- reputational harm; and
- immigration or travel consequences, particularly if the offence is deportable or where extradition has been defeated.

The human element: client-centred lawyering 18.8

Individual representations raise unique issues concerning client-centred lawyering beyond those that typically arise in a corporate representation. Criminal actions are particularly traumatic for both clients and their families, especially because most white-collar clients are interacting with the criminal justice system for the first time in their lives. While the luxury of time is not always available, counsel should strive to allow the client enough of it to process the situation before making any irreversible decisions.

Counsel also must be attuned to the impact of the proceeding on the client's physical and mental health. Preliminary discussions should cover these issues, as well as the client's support system. Engaging with the client's support system is essential at all stages, including fact gathering, assessing strategic options, deploying financial resources and determining resolution. For clients facing criminal proceedings, family support impacts all aspects of the case, from bail conditions to the sentence imposed.

Finally, counsel must be sensitive to the impact of the proceeding on the client's professional and personal reputation. Even if no enforcement action is taken, mere association with a proceeding – particularly if criminal – may so negatively impact the client's reputation that he or she is unable to work in the industry again or live in the same community.[124] Counsel should be prepared to advise clients on how to mitigate reputational risks and expect that these considerations will impact clients' decisions.

See Chapter 39 on publicity

Civil Forfeiture Complaint in COVID-19 Fraud Case' (10 Jun. 2020), https://www.justice.gov/usao-wdva/pr/us-files-civil-forfeiture-complaint-covid-19-fraud-case.

124 Reputational concerns are likely to be heightened when the proceeding is high-profile and the client faces media inquiries. While clients may wish to hire a public relations firm, any decision to engage a third party should be carefully considered in light of the fact that those communications are often not privileged and could adversely affect the outcome of the proceeding. See, e.g., *Haugh v. Schroder Inv. Mgmt. N. Am. Inc.*, No. 02-7955, 2003 WL 21998674, at *3 (S.D.N.Y. 25 Aug. 2003).

© Law Business Research 2021

19

Whistleblowers: The UK Perspective

Alison Wilson, Sinead Casey, Elly Proudlock and Nick Marshall[1]

19.1 Introduction

Recent years have seen an increasing focus on whistleblowing as a cornerstone of good corporate culture, particularly in the financial services sector where a key feature of the Senior Managers and Certification Regime (SMCR) is a requirement for firms to appoint a 'whistleblowers' champion'. Effective whistleblowing procedures can allow problems to be identified early, providing an opportunity to rectify shortcomings and to prevent a crisis. Whistleblowing can also allow businesses to manage market-notification obligations and public relations, identify poor performance and potentially avoid costly employment litigation.

19.2 The legal framework

19.2.1 Employment Rights Act 1996

Whistleblowing legislation was introduced in 1998 following the realisation that a number of high-profile disasters may have been prevented or their effect reduced if a worker had spoken up, or their employer had listened to them.[2] Amendments to the Employment Rights Act 1996 (ERA) came into force in July 1999,[3] providing two key protections for whistleblowers: unlawful detri-

1 Alison Wilson and Sinead Casey are partners, Elly Proudlock is counsel, and Nick Marshall is a managing associate at Linklaters LLP. The authors wish to acknowledge the contribution of Peter Binning, a partner at Corker Binning, and Elisabeth Bremner, a partner at CMS Cameron McKenna Nabarro Olswang LLP, for their contributions to a previous version of this chapter.

2 For example, the Zeebrugge ferry disaster in 1987, the Clapham rail crash in 1988 and the BCCI collapse in 1992.

3 Introduced by the Public Interest Disclosure Act 1998 (PIDA).

© Law Business Research 2021

ment (protecting employees and workers, including some limited liability partnership members,[4] and even judicial office holders[5]) and automatically unfair dismissal (protecting employees). There is no qualifying length of service for bringing whistleblowing claims.

Unlawful detriment 19.2.1.1

Subjecting a worker to a detriment because they have made a protected disclosure is unlawful. Detriments include, but are not limited to, pay cuts, limiting career prospects and disciplinary action. Detriments after termination of employment also qualify,[6] so employers should proceed cautiously when drafting references.

Automatically unfair dismissal 19.2.1.2

Dismissing an employee who has blown the whistle is automatically unfair if the reason, or principal reason, for the dismissal is that they have made a protected disclosure. Since compensation for successful whistleblowing unfair dismissal claims is uncapped, compensation can be high – especially if the individual encounters difficulty finding a new job because of the dismissal.

Qualifying disclosures 19.2.1.3

Six categories of disclosure are protected as 'qualifying disclosures'. The disclosure must, in the worker's reasonable belief, tend to show that one or more of the following failures has occurred or is likely to occur:

- a criminal offence;
- breach of a legal obligation;
- a miscarriage of justice;
- danger to the health and safety of any individual;
- damage to the environment; or
- the deliberate concealment of information about any of the above.

Since 2013, to make a qualifying disclosure the worker must reasonably believe that the disclosure is in the public interest.[7] 'Public interest' is not defined, but in *Chesterton Global and Verman v. Nurmohamed*,[8] the Court of Appeal decided

4 In *Clyde & Co LLP v. Bates van Winkelhof* (2014) UKSC 32, the Supreme Court held that a former equity partner of a law firm incorporated as a limited liability partnership (LLP) was a worker under s.230(3) Employment Rights Act 1996 and therefore eligible to bring a whistleblowing claim against the LLP.

5 In *Gilham v. Ministry of Justice* (2019) UKSC 44, the Supreme Court found that a district judge falls within the definition of 'worker' under ERA. It would amount to unlawful discrimination based on occupational status contrary to Article 14 (read with Article 10) of the European Convention on Human Rights if such a reading were not given to the definition of 'worker'.

6 *Woodward v. Abbey National Plc* (2006) EWCA Civ 822.

7 Enterprise and Regulatory Reform Act 2013, s.17 amended ERA at s.43B(1).

8 (2017) EWCA Civ 979.

© Law Business Research 2021

that the interests served by the disclosure do not have to extend outside the workplace. Four considerations are relevant:

- the number of people affected by the disclosure;
- the nature of the interests affected and the extent to which those interests are affected by the wrongdoing disclosed;
- the nature of the wrongdoing disclosed; and
- the identity of the alleged wrongdoer.

Anything that affects a class of people could be caught. 'Everyday' employment disputes over contractual terms (for example, remuneration) may have a public interest element, especially where these have serious implications or impact large numbers of people. Issues such as discrimination or equal pay at work might also have a public interest element.

Provided workers believe, acting reasonably, that the relevant failure has occurred or is likely to occur, they will be protected even if their belief turns out to be wrong.[9] For a belief to be 'reasonable' it must be founded in more than unsubstantiated rumour or opinion.

There is no requirement for the disclosure to be 'in good faith'. However, if an employment tribunal finds that a disclosure was made in bad faith, it can reduce compensation by up to 25 per cent. Disclosures made predominantly for personal interest or with malice are not usually in 'good faith'.[10]

19.2.1.4 Vicarious and personal liability

Vicarious liability

Employers may be vicariously liable for detriments caused to a worker by co-workers (and in some cases by agents of the employer) on grounds that the worker made a protected disclosure.[11]

The employer will have a defence if it took all reasonable steps to prevent the detrimental treatment; such steps would include having an appropriate whistleblowing policy and providing training.

Personal liability

Claimants can pursue individuals personally for liability arising from whistleblowing detriments. Doing so is often tactical. In *Timis and another v. Osipov*,[12] the Court of Appeal held that two non-executive directors were jointly and severally liable for the losses flowing from Mr Osipov's dismissal (totalling approximately £1.75 million).

9 *Babula v. Waltham Forest College* (2007) EWCA Civ 174.

10 *Bachnak v. Emerging Markets Partnership Europe* (2006) UKEAT/0288/05/RN.

11 Employment Rights Act 1996, s.47B(1A)-1(E).

12 [2018] EWCA Civ 2321.

© Law Business Research 2021

Legislative proposals 19.2.2

In October 2019, the Council of the European Union formally adopted the Whistleblower Directive,[13] which had to be implemented by Member States by December 2021.

Following its departure from the European Union, the United Kingdom is not required to implement the Whistleblower Directive. Despite Protect,[14] the whistleblowing charity, urging the UK government to bring the new provisions into domestic law, there are no proposals to do so. A bill proposing the creation of an Office for the Whistleblower was presented to Parliament in May 2021.[15]

Non-disclosure agreements and whistleblowing 19.2.3

A non-disclosure agreement (NDA) – a contractual commitment that a party (or parties) will keep certain information confidential – is commonly included in settlement agreements between employers and departing employees. Under an NDA, confidentiality may attach to the terms of the settlement agreement and to the amount of any sums paid under it, as well as to the underlying complaints that the employee made. If the NDA is breached, the other party can seek damages for breach of contract.

In the wake of the #MeToo movement, the use of NDAs by employers has come under the spotlight and has been criticised as a means of silencing whistleblowers. In July 2019, the All-Party Parliamentary Group for Whistleblowing urged the government to ban the use of NDAs in whistleblowing cases.[16]

Any NDA clause designed to prevent a worker from making a whistleblowing disclosure is void under section 43J of the ERA and unenforceable. Seeking to rely on an NDA to prevent whistleblowing disclosures could amount to an unlawful detriment against the employee or worker, as well as risking additional adverse publicity if the issue becomes public.

Firms authorised by the Financial Conduct Authority (FCA) are under specific obligations when it comes to settlement agreements with workers. Lawyers advising clients on NDAs must also consider their professional obligations.

FCA/PRA systems and controls requirements 19.2.4

Both the FCA and the Prudential Regulation Authority (PRA) require firms to implement and maintain appropriate and effective internal whistleblowing

13 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting on breaches of European Union law.

14 Previously known as Public Concern at Work. See https://protect-advice.org.uk/.

15 In addition to Protect's Bill to Strengthen Whistleblowing Protection, Baroness Kramer of the All-Party Parliamentary Group introduced the Office of the Whistleblower Bill.

16 See https://www.appgwhistleblowing.co.uk/.

© Law Business Research 2021

arrangements as part of an effective risk management system.[17] The FCA's rules and guidance are contained in SYSC 18 of its Handbook, which applies to SMCR banking and insurance sector firms and also serves as non-binding guidance to all other firms authorised under the Financial Services and Markets Act 2000 (FSMA). The PRA's rules are higher level and found in the PRA Rulebook.

The SYSC 18 requirements fall into four categories:

- maintenance of appropriate and effective arrangements for whistleblowing;[18]
- appointment of a whistleblowers' champion;[19]
- settlement agreements with workers;[20] and
- whistleblowing obligations under the MiFID regime and other sectoral legislation.[21]

19.2.4.1 Maintaining appropriate internal whistleblowing arrangements

While firms are required to establish, implement and maintain appropriate and effective arrangements for the disclosure of reportable concerns (including concerns related to suspected market abuse) by whistleblowers, neither regulator has prescribed what the arrangements should be. The regulators recognise that whistleblowing arrangements may vary between firms[22] and that firms may use third parties to provide aspects of their whistleblowing services, with appropriate quality controls and monitoring.

The arrangements that a firm has in place should allow effective escalation of reportable concerns, including to the FCA and PRA. A firm's arrangements should also:

- allow for disclosure to be made through a variety of means (e.g. through an online system, a telephone hotline, a third-party provider or a designated team);
- handle a whistleblower's request for confidentiality or anonymity;
- include reasonable measures to ensure whistleblowers are not victimised;
- provide feedback to whistleblowers on their concerns, where appropriate and feasible;
- include record-keeping of reportable concerns;
- include maintenance of up-to-date whistleblowing policies and procedures that are readily available to the firm's employees;
- allow for the preparation of an annual report to the firm's governing body on the effectiveness and operation of the firm's processes;
- include relevant training;

17 FCA Handbook, SYSC 18.3.1(1)R; and, for example, PRA Rulebook Whistleblowing rule 2A.2(1) of the General Organisational Requirements section for CRR firms.

18 FCA Handbook, SYSC 18.3.

19 ibid., SYSC 18.4.

20 ibid., SYSC 18.5.

21 ibid., SYSC 18.6.

22 Whistleblowing in deposit-takers, PRA designated investment firms and insurers – SS39/15 (Supervisory Statement, October 2015, updated July 2018).

© Law Business Research 2021

- include reporting to the FCA and PRA if firms lose an employment tribunal claim based on detriment suffered from making a protected disclosure; and
- ensure UK employees are made aware of the FCA's and PRA's whistleblowing services and that they can approach either regulator direct without first raising a concern internally.[23]

The whistleblowers' champion 19.2.4.2

A key component of the SMCR is a requirement for firms to appoint a whistleblowers' champion with responsibility for ensuring and overseeing the integrity, independence and effectiveness of the firm's policies and procedures on whistleblowing. The FCA expects that this role will be filled by a non-executive director.[24]

The FCA and PRA have not been prescriptive about how whistleblowers' champions should perform their role, and have acknowledged that firms are likely to take different approaches depending on their structure and size.[25]

Settlement agreements with workers 19.2.4.3

The FCA's rules require a firm to include in a settlement agreement with a worker a term making clear that nothing in that settlement agreement prevents the worker from making a protected disclosure.[26]

Competition and Markets Authority and whistleblowers 19.2.5

In exceptional circumstances, the Competition and Markets Authority (CMA) offers rewards of up to £100,000 for information about cartel activity. The rewards are provided at the discretion of the CMA subject to factors including the value of the information, the harm done to consumers and the risk the whistleblower has taken to provide the information.[27] The CMA actively encourages whistleblowing and self-reporting through various campaigns and through its leniency regime.

Serious Fraud Office and online whistleblowing 19.2.6

The SFO's reporting service enables the reporting of information about serious fraud, bribery or corruption – whether as a whistleblower or on behalf of a company making a self-report. Whistleblowers are initially encouraged to

See Chapter 3 on self-reporting to authorities

23 Retail and Wholesale Banking: review of firms' whistleblowing arrangements (Policy Statement, November 2018).

24 FCA Handbook, SYSC 18.4.1(4)G.

25 Whistleblowing in deposit-takers, PRA designated investment firms and insurers – FCA CP15/4, PRA CP6/15 (FCA/PRA Consultation Paper, February 2015)

26 FCA Handbook, SYSC 18.5.1R. A *pro forma* clause is provided in SYSC 18.5.2.

27 The CMA's published policy on rewards for information about cartels is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/299411/Informant_rewards_policy.pdf.

© Law Business Research 2021

follow the whistleblowing procedures in their own organisation if they suspect wrongdoing. If the whistleblower is not comfortable, or there are no procedures, then they should approach the SFO or another prescribed body.[28]

19.2.7 Human rights

Demonstrating respect for human rights is increasingly important for businesses. Since 2011 when the United Nations endorsed the UN Guiding Principles on Business and Human Rights (UNGPs),[29] 'soft law' standards encouraging companies to manage more closely their human rights risks and impacts across their operations and supply chains have proliferated. The UNGPs require businesses to avoid infringing others' human rights and to address adverse impacts on human rights they are involved with. Their frequent adoption by companies has led to increasing NGO, investor and wider stakeholder scrutiny.

Beyond soft law instruments, we have seen laws introduced that require companies to report on human rights. For example, section 54 of the Modern Slavery Act 2015 requires in-scope companies to produce a slavery and human trafficking statement each financial year on the steps they have taken to ensure slavery and human trafficking are not taking place in their supply chains and business.[30] Section 414CA of the Companies Act 2006[31] requires certain large companies to prepare a non-financial information statement containing information on their respect for human rights and a description of their policies in this regard.

Most recently, several European countries have introduced or are considering mandatory regimes with substantive requirements on conducting due diligence.[32]

Businesses have realised that, to fulfil their obligations to respect human rights under the UNGPs and comply with applicable legislative regimes, they need to review their policies and procedural frameworks to ensure they

28 See https://www.sfo.gov.uk/publications/information-victims-witnesses-whistleblowers/#whistleblowers.

29 UN High Commissioner for Refugees, Guiding Principles on Business and Human Rights, 2011, available at https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf.

30 This requirement has since been replicated by similar regimes or proposals in other jurisdictions, such as Australia.

31 Inserted by The Companies, Partnerships and Groups (Accounts and Non-Financial Reporting) Regulations 2016 published in 2016 as part of the UK government's implementation of Directive 2014/95/EU of the European Parliament, commonly known as the 'EU Non-Financial Reporting Directive' or 'NFRD'.

32 Such requirements were originally introduced in France with the 2017 Devoir de Vigilance and have since been replicated in other jurisdictions. For example, a law on child labour due diligence has been introduced in the Netherlands and the European Commission announced in April 2020 that it would introduce mandatory human rights diligence for EU companies in 2021. At the time of writing, this is expected by mid-December 2021.

© Law Business Research 2021

understand their potential human rights risks and impacts. Many companies have implemented whistleblowing policies to support the management of human rights and supply-chain risk, which is recommended in Home Office guidance.[33] It is best practice for a whistleblowing mechanism to be open to all workers (including contractors) rather than just employees. Companies have therefore increasingly opened up their processes to those in their supply chains, particularly where they are involved in high-risk activities or jurisdictions.

It is also important to recognise the potential human rights consequences if the procedures do not contain sufficient whistleblower protections. This can include the rights to privacy and freedom of speech, protected under Articles 8 and 10 of the European Convention on Human Rights (ECHR), or, in the worst case, the right to life (ECHR, Article 1). Human rights considerations should underpin the design and operation of an effective whistleblowing regime, and companies should ensure that, in implementing procedures to identify human rights impacts and risks in their operations and supply chain, they are not creating new ones.

The corporate perspective: representing the firm 19.3

Responsibility for whistleblowing among senior managers under SMCR 19.3.1

When representing a regulated firm involved in a whistleblowing investigation, regard must be had both to the firm's compliance with the systems and controls requirements outlined above and to individual managers' personal SMCR obligations.

The SMCR requires most individuals employed in the UK banking and insurance sectors to adhere to the FCA's and PRA's Individual Conduct Rules.[34] Senior managers must also comply with the Senior Manager Conduct Rules, while non-executive directors (who are not themselves senior managers) are subject to Senior Manager Conduct Rule 4 as well as the Individual Conduct Rules. On 9 December 2019, the SMCR was extended to certain other financial services firms, including asset management firms and non-bank mortgage lenders. Certain individual rules may require the relevant individuals to disclose information to the regulators. In the context of whistleblowing, this means that information received via internal whistleblowing channels may, in turn, need to be escalated to the appropriate regulator.

33 UK Home Office, 'Transparency in Supply Chains etc. – A practical guide', p. 29, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/649906/Transparency_in_Supply_Chains_A_Practical_Guide_2017.pdf.

34 See Code of Conduct (COCON) 2.1, FCA Handbook.

© Law Business Research 2021

19.3.1.1 Individual Conduct Rules

The FCA/PRA Individual Conduct Rule 3 stipulates that relevant individuals must be open and co-operative with the FCA, the PRA and other regulators with appropriate jurisdiction. The FCA's Code of Conduct Handbook (COCON) provides specific guidance as to what this rule requires.

COCON 4.1.10 provides guidance that there is no duty on a person to report information directly to the regulator concerned unless they are one of the persons responsible in the firm for reporting matters to the regulator (although if a person takes steps to influence the decision not to report or acts in a way that is intended to obstruct the reporting of the information to the regulator, they will be treated as if they had taken on responsibility for deciding whether to report that matter).

Those operating a whistleblowing function will not automatically assume direct responsibility for escalating reportable concerns to the regulator. However, firms should ensure that appropriate arrangements are in place so that those responsible for regulatory reporting are informed on a timely basis of issues likely to be of interest to the regulator identified through the whistleblowing channels.

19.3.1.2 Senior Manager Conduct Rules

The FCA/PRA Senior Manager Conduct Rule 4 requires senior managers and non-executive directors to disclose appropriately any information of which the FCA, PRA or other regulator with appropriate jurisdiction would reasonably expect. While there is overlap between FCA/PRA Senior Manager Conduct Rule 4 and Individual Conduct Rule 3, COCON 4.2.26 makes clear that these are distinct obligations, with Senior Manager Conduct Rule 4 requiring proactive disclosure rather than just accurate responses to regulatory enquiries. COCON 4.2.28 clarifies that senior managers (or non-executive directors) need not report information outside the scope of their responsibility. However, once they become aware of the information (including through whistleblowing) they should make enquiries to satisfy themselves that it is being dealt with by the appropriate individual.

19.3.1.3 Approved persons

Since December 2019, solo-regulated firms previously governed by the approved persons regime have been governed by the SMCR.

19.3.2 Whistleblowing in adequate or reasonable systems and controls

19.3.2.1 Bribery Act 2010 and adequate procedures

See Chapter 28 on extraterritoriality

Under section 7 of the Bribery Act 2010, a company can be criminally liable for failing to prevent bribery by one of its associated persons.

© Law Business Research 2021

It is a defence for a company to show that it had adequate prevention procedures in place.[35] Such procedures are likely to include procedures for the reporting of bribery including 'speak up' or 'whistleblowing' procedures.[36]

Criminal Finances Act 2017 and reasonable procedures 19.3.2.2

Under sections 45 and 46 of the Criminal Finances Act 2017, a company can be criminally liable for failing to prevent the facilitation of tax evasion offences by its associated persons.

It is a defence for a company to show that it had reasonable prevention procedures in place. Such procedures are likely to include protection for whistleblowers.[37] In February 2019, HMRC launched an online reporting form for authorised representatives to self-report a failure to prevent the facilitation of tax evasion on the part of their organisation.

See Chapter 3 on self-reporting to authorities

Changing regulatory expectations 19.3.3

In November 2018, following its review of firms' whistleblowing arrangements in the retail and wholesale banking sector, the FCA published examples of good practice and areas for improvement with respect to policies and procedures, the role of the whistleblowers' champion and the annual whistleblowing report and training.[38] These published examples are a useful reference point for companies assessing the efficacy of their arrangements, including as to protection against victimisation.

In May 2019, the FCA published its industry feedback with respect to wholesale banking.[39] It identified several practices as examples of 'encouraging' whistleblowing initiatives implemented by firms, including:

- engagement by managers and staff directly with a whistleblower to understand fully what he or she would like to achieve and make a sustained effort to manage appropriately the whistleblower's expectations;
- outsourcing of analysis on all whistleblowing cases to ensure fair and confidential treatment;
- detailed end-to-end reviews of the process for whistleblowing events involving all disciplines (e.g., HR, legal, compliance, business heads) to make it more transparent, fairer and quicker;
- creation of a 24-hour, multilingual hotline for anonymous escalations; and

35 Bribery Act 2010, s.7(2).

36 Ministry of Justice, The Bribery Act 2010: Guidance, para. 1.7, available at https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

37 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf, at p. 23.

38 Retail and Wholesale Banking: review of firms' whistleblowing arrangements (first published 14 Nov. 2018), available at www.fca.org.uk/publications/multi-firm-reviews/retail-and-wholesale-banking-review-firms-whistleblowing-arrangements.

39 See 'Progress and challenges' Industry Feedback for 2018/2019 Wholesale Banking Supervision (FCA, May 2019).

© Law Business Research 2021

- discreet monitoring for a minimum of three years following a whistleblowing event, to ensure a whistleblower was not treated badly as a consequence of their disclosure.

In the FCA's subsequent industry feedback for wholesale banking published in September 2020, the FCA noted that firms' internal whistleblower channels were largely unused and reserved for the most serious cases. The FCA also observed a persistent and significant lack of psychological safety in day-to-day 'speak up and challenge', which firms would need to address.[40]

As part of its continued focus on culture, the FCA is particularly interested where whistleblowing allegations are raised against those designated as senior managers or material risk takers, being those with the greatest potential to cause harm to a firm's customers or the markets in which it operates. A number of firms have undertaken to notify the FCA of such allegations immediately on receipt and before investigation.

The FCA has also made clear that it views a lack of diversity and inclusion and non-financial misconduct as obstacles to creating an environment in which it is safe to speak up.[41] Whistleblowing acts as an important barometer for the FCA and PRA to test an organisation's culture and purpose.

Outside the financial regulatory sector, listed companies are required under the UK Corporate Governance Code 2018 to ensure that members of the workforce can raise concerns in confidence (and anonymously if they wish). The board should ensure that arrangements are in place for the proportionate and independent investigation of such matters and for follow-up action.

19.3.4 Practical considerations

19.3.4.1 Effective reporting channels and protecting anonymity

A whistleblowing policy should detail the process of making internal disclosures and should be disseminated across the organisation through regular communications and training that encourage a 'speak up' culture. Ideally there should be a range of channels through which disclosures can be made.

In June 2020, Protect published its second edition of 'Silence in the City', an analysis of the experience of whistleblowing in the financial services sector. The study found that steps taken in the sector to embed trust in internal whistleblowing arrangements were working, with 93 per cent of whistleblowers raising their concerns internally (a significant increase from the 78 per cent in

40 See 'Messages from the Engine Room' Industry Feedback for 2019/2020 Wholesale Banking Supervision (FCA, September 2020).

41 https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-non-financial-misconduct-wholesale-general-insurance-firms.pdf?LinkSource=PassleApp.

© Law Business Research 2021

their first report).[42] Despite this progress, there is significant work to be done to embed processes that protect the identity of whistleblowers. Protect found that 70 per cent of whistleblowers were either victimised, dismissed or felt that resignation was the only option available to them.[43]

Conduct of the investigation 19.3.4.2

Internal investigations involving whistleblower allegations require careful handling because of the reputational and employment law consequences that may follow if a whistleblower is not afforded the required legal protections.

See Chapter 5 on beginning an internal investigation

Consideration should be given as to whether to offer whistleblowers independent legal representation.

See Chapter 7 on witness interviews

Where possible the whistleblower should be kept informed about the progress of the investigation, although care should be taken not to take any steps that might result in a loss of privilege or confidentiality. Expectations should be effectively managed and care taken not to promise outcomes that may not be deliverable. For example, a whistleblower's desire to remain anonymous may place constraints on the extent to which the allegations can be investigated.

See Chapter 36 on privilege

Data protection 19.3.4.3

A whistleblowing process will inevitably involve the processing of personal data and so must comply with the Data Protection Act 2018 and the UK GDPR.[44] However, it is still important to ensure that the whistleblowing process, and any subsequent investigation, complies with the GDPR. Particular issues to consider include keeping the whistleblowing information secure and limiting access to it, setting an appropriate retention period, not collecting excessive amounts of personal data, being alert to the right of individuals to access a copy of their personal data and, at least in general terms, being transparent about the operation of the whistleblowing process. It may also be necessary to conduct a data protection impact assessment.[45]

See Chapter 40 on data protection

42 Silence in the City 2, Protect, June 2020, p. 7, at https://s3-eu-west-1.amazonaws.com/public-concern-at-work/wp-content/uploads/images/2020/06/19125704/Protect-SILENCE-IN-THE-CITY-2-2020.pdf.

43 Id.

44 The UK GDPR means the EU General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018, s.3. The substantive obligations under the UK GDPR are broadly the same as those under the EU GDPR.

45 In particular, the UK Information Commissioner has identified whistleblowing hotlines as a type of processing that might necessitate a data protection impact assessment. See "Examples of processing 'likely to result in high risk' available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/.

© Law Business Research 2021

19.3.4.4 Interaction with regulatory obligations

Principle 11/Fundamental Rule 7

Firms must deal with their regulators in an open and co-operative way and proactively disclose anything relating to the firm of which the regulators would reasonably expect notice. Information that comes to light via a whistleblowing report may therefore have to be escalated to the relevant authority. In accordance with the FCA's Supervision Manual, firms must notify the FCA of matters having a serious regulatory impact. This includes any matter that could have a significant adverse impact on the firm's reputation.[46] In the current regulatory climate there may be an expectation that whistleblowing reports against senior managers or allegations of serious sexual harassment or other forms of serious non-financial misconduct will be disclosed immediately.

Proceeds of Crime Act 2002

Those in receipt of whistleblower reports will need to consider whether the information disclosed triggers any money laundering reporting obligation under the Act (for those in the regulated sector) or it is necessary to seek a defence against money laundering from the NCA to deal with certain property.

See Chapter 3 on self-reporting to authorities

Considerations for listed companies

When receiving whistleblowing reports, listed companies should also have regard to their disclosure obligations under the Disclosure Guidance and Transparency Rules and the UK Market Abuse Regulation.[47] In accordance with Section 2.2 of the rules and Article 17(1) of the regulation, for example, listed companies must disclose inside information to the market as soon as possible.

19.3.4.5 Cross-border considerations

See Chapters 3 on self-reporting and 40 on data protection

Exchange of information in relation to whistleblowers or disclosures

Data protection issues will need to be considered in the context of any transfer of data overseas.

Territorial application of UK whistleblower legislation

A tribunal can only hear a whistleblowing claim against a British employer brought by an employee working abroad if there is a stronger connection with Britain or British employment law than with the country in which they are working. In *Foreign and Commonwealth Office (FCO) v. Bamieh*,[48] the Court of Appeal held that an employment tribunal had no territorial jurisdiction to hear

46 See FCA Supervision Manual 15.3.1(2)R.

47 See Disclosure Guidance and Transparency Rules, FCA Handbook, Disclosure Guidance and Transparency Rules sourcebook.

48 (2019) EWCA Civ 803.

© Law Business Research 2021

whistleblowing detriment claims brought by an FCO employee working in Kosovo against co-workers who were also employed by the FCO and working in Kosovo. The focus should be on the relationship between the claimant and the co-workers rather than on the relationship between the co-workers and the employer. The individuals concerned having a common employer is not sufficient to give the tribunal jurisdiction.

The individual perspective: representing the individual 19.4

Legal risks associated with whistleblowing 19.4.1

A decision to make a whistleblowing disclosure can have far-reaching consequences and requires a careful assessment of the legal risks. Despite the protections afforded by the ERA, whistleblowers may be exposed to the risk of criminal investigation or prosecution if they are personally implicated in the conduct disclosed. Those in regulated professions may be vulnerable to regulatory or disciplinary action by their regulators or professional bodies. Where the matter potentially spans more than one jurisdiction, individuals will need to remember that different jurisdictions apply different whistleblower protection standards. Advice on local employment and possibly criminal laws should be sought where necessary.

Whistleblowers might also commit criminal offences in the course of obtaining information to support their disclosures. Such offences might include securing unauthorised access to computer material,[49] unlawfully obtaining personal data,[50] unlawful interception of communications,[51] theft or even fraud. Whistleblowers may also be vulnerable to civil actions for breach of confidence.

Serious Organised Crime and Police Act 2005: immunity and leniency 19.4.2

Where an individual faces criminal liability, they may be able to obtain immunity from prosecution. Section 71 of the Serious Organised Crime and Police Act 2005 (SOCPA) empowers most criminal prosecutors to offer an individual immunity from prosecution by issuing a written immunity notice. This power is used rarely and only in very exceptional circumstances.

As an alternative, section 73 of SOCPA provides that if an offender pleads guilty and offers assistance to an investigator or prosecutor, the sentencing court may pass a reduced sentence to reflect that assistance.

See Chapter 17 on individuals in cross-border proceedings

49 Computer Misuse Act 1990, s.1.

50 Data Protection Act 2018, ss.170 and 196. The specific public interest defence to s.170 of the Data Protection Act 1980 (under s.170(2)(c)) may well be tested in a data breach of images taken from the Department of Health and Social Care CCTV system in 2021. See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/statement-on-ico-investigation-into-department-of-health-and-social-care-cctv-footage/.

51 Investigatory Powers Act 2016, s.3(1).

© Law Business Research 2021

19.4.3 Professional obligations

Regulated professionals may have a duty to report certain information to the appropriate regulator. For example, FCA/PRA Senior Manager Conduct Rule 4 requires senior managers and non-executive directors to disclose appropriately any information of which the FCA, PRA or other regulator with appropriate jurisdiction would reasonably expect notice.

In March 2018, the Solicitors Regulatory Authority (SRA) issued a warning notice to legal professionals in relation to the use of NDAs,[52] which sets out the obligations that exist when a law firm is considering an NDA with a person who has made a complaint about misconduct within a law firm, or when legal professionals are advising clients on NDAs with individuals. The warning notice states that legal professionals (and those responsible for managing complaints within law firms) should ensure that they do not:

- use NDAs in circumstances in which the subject of the NDA may, as a result of its use, feel unable to notify the SRA or other regulators or law enforcement agencies of conduct that might otherwise be reportable;
- fail to notify the SRA of misconduct, or a serious breach of regulatory requirements, by any person or firm, including wrongdoing by the firm or harassment or other misconduct towards others such as employees or clients; or
- use NDAs as a means of improperly threatening litigation or other adverse consequences, or otherwise exerting inappropriate influence over people not to make disclosures which are protected by statute, or reportable to regulators or law enforcement agencies.

Inappropriate use of NDAs may constitute a breach of the SRA's Standards and Regulations and lead to disciplinary action.

Further SRA guidance[53] reiterates the SRA's previous warning that those regulated by the SRA must not attempt to prevent anyone from making a complaint or providing information to the SRA, or any other body exercising regulatory, investigatory or prosecutorial functions in the public interest.

19.4.4 Practical questions

19.4.4.1 To whom to blow the whistle

An individual will need to carefully consider whether to blow the whistle externally because this may result in the loss of statutory protection. To be a protected disclosure, the whistleblower must make a qualifying disclosure to an appropriate person or organisation.

52 See https://www.sra.org.uk/solicitors/guidance/warning-notices/use-of-non-disclosure-agreements-ndas--warning-notice/, as updated on 25 November 2019.

53 See https://www.sra.org.uk/solicitors/guidance/ethics-guidance/reporting-notification-obligations/, published on 25 November.

© Law Business Research 2021

In most cases, disclosures should be made to the employer. However, in some circumstances individuals may be protected if they disclose information externally.

Parliament has approved a list of 'prescribed persons' to whom a worker or an employee can make a disclosure, provided they believe the information is substantially true and concerns a matter within that person's area of responsibility. They include the FCA, the PRA, the SFO, the NCA, HMRC, the Health and Safety Executive and the CMA. There is no requirement to alert the employer beforehand.

Where the worker or employee reasonably believes a third party (such as a client or supplier) is responsible for the wrongdoing, they can report it to that third party without telling the employer.

Disclosure to other external sources (e.g. the media) is protected only if the individual believes that the information is substantially true and they do not act for gain. Unless the matter is 'exceptionally serious', they must have already disclosed it to the employer or a prescribed person (or believe that, if they did, evidence would be destroyed or they would suffer reprisals). Disclosure to that person must also be reasonable.

Requests to sign an NDA 19.4.4.2

Any request to sign an NDA purporting to prevent an individual from raising whistleblowing concerns should be resisted and will be unenforceable.

Challenges to unfair treatment of whistleblowers 19.4.4.3

An individual who is a worker or employee and who is subjected to unfair treatment by their employing or engaging entity or by other employees or co-workers may have a claim in the employment tribunal against individuals and the entity.

© Law Business Research 2021

20

Whistleblowers: The US Perspective

Daniel Silver and Benjamin A Berringer[1]

20.1 Overview of US whistleblower statutes

The US legal system contains a multitude of state and federal laws that protect individuals who report potential misconduct (whistleblowers) from retaliation for making the report.[2] Some of these laws protect specific classes of individuals, such as truck drivers,[3] nuclear engineers,[4] pilots[5] and miners.[6]

1 Daniel Silver is a partner and Benjamin A Berringer is an associate at Clifford Chance US LLP.

2 The exact nature of this protection depends significantly on the statute that creates the protection. For example, the Surface Transportation Assistance Act states that 'a person may not discriminate' against truck drivers and certain other employees 'regarding pay, terms, conditions, or privileges of employment' for making a whistleblower report. 49 U.S.C. § 31105. On the other hand, the Sarbanes-Oxley Act prohibits a broader range of conduct, but applies to a narrower class of employers. See infra notes 17 to 24 and accompanying text.

3 The Surface Transportation Assistance Act protects truck drivers and certain other employees from retaliation for reporting violations of regulations related to the safety of commercial vehicles. 49 U.S.C. § 31105.

4 The Energy Reorganization Act protects employees of operators, contractors and subcontractors of nuclear power plants licensed by the Nuclear Regulatory Commission from retaliation for reporting violations of the Atomic Energy Act of 1954. 42 U.S.C. § 5851.

5 The Federal Airline Deregulation Act's Whistleblower Protection Program protects employees of air carriers, their contractors and their subcontractors from retaliation for, inter alia, reporting violations of laws related to aviation safety. 49 U.S.C. § 42121.

6 The Federal Mine Safety and Health Act of 1977 prohibits employment discrimination against a 'miner, representative of miners or applicant for employment in any coal or other mine' as a reprisal for making safety-related complaints. 30 U.S.C. § 815.

© Law Business Research 2021

Others relate to specific conduct such as motor vehicle safety issues,[7] violations of the Clean Air Act,[8] violations of the Clean Water Act,[9] violations of the Anti-Money Laundering Act[10] or violations of the Affordable Care Act.[11] Each of these laws is structured differently. As a result, the precise steps that a whistleblower must take to file a report, whether the whistleblower has a private right of action and the scope of protection may vary depending on the statutory basis for the whistleblower claim.[12]

The SEC whistleblower regimes 20.1.1

US securities laws protect whistleblowers who report potential misconduct by entities and individuals subject to regulation by the US Securities and Exchange Commission (SEC). This protection was originally created by the Sarbanes-Oxley Act (SOX) in 2002. It was then strengthened and expanded by the Dodd-Frank Act (DFA) in 2009, which created the Whistleblower Protection Program (the Program), pursuant to which individuals who voluntarily report 'original information'[13] about potential violations of federal securities laws are protected from retaliation and entitled to a financial award if the information leads to a successful judicial or administrative enforcement

7 The Moving Ahead for Progress in the 21st Century Act prohibits discrimination by motor vehicle manufacturers, part suppliers and dealerships against employees who provide information about any motor vehicle defect or violation of the Motor Vehicle Safety Act. 49 U.S.C. § 30171.

8 The Clean Air Act contains a provision protecting employees from retaliation for reporting violations of the Act. 42 U.S.C. § 7622.

9 The Water Pollution Control Act contains a provision protecting employees from retaliation for reporting violations of the Act. 33 U.S.C. § 1367.

10 The Anti-Money Laundering Act contains a provision protecting employees from retaliation for reporting violations of the Act. 31 U.S.C. § 5323(g).

11 The Affordable Care Act protects employees from retaliation for reporting violations of certain of its provisions, including, inter alia, discrimination based on an individual's receipt of health insurance subsidies, denial of coverage for a pre-existing condition and an insurer's failure to rebate a portion of an excess premium to customers. 29 U.S.C. § 218c.

12 Compare, e.g., 42 U.S.C. § 7622 (no private cause of action for whistleblower retaliation under the Clean Air Act), with 29 U.S.C. § 1132(a) (creating a private cause of action for the enforcement of ERISA provisions, including anti-retaliation provisions).

13 The US Securities and Exchange Commission (SEC) has defined original information as 'information derived from your independent knowledge (facts known to you that are not derived from publicly available sources) or independent analysis (evaluation of information that may be publicly available but which reveals information that is not generally known) that is not already known by us.' SEC, Office of the Whistleblower, Frequently Asked Questions, https://www.sec.gov/about/offices/owb/owb-faq.shtml. The SEC has also stated that information from certain individuals, including attorneys and fiduciaries, may not be deemed original. See infra notes 80 to 82 and accompanying text.

© Law Business Research 2021

action in which the SEC obtains monetary sanctions over US$1 million.[14] The Program has been a significant success for the SEC. Since August 2011, the Program has received over 52,400 whistleblower reports from individuals in all 50 US states and 133 foreign countries.[15] In fiscal year 2021 alone, the SEC received over 12,200 whistleblower reports, including over 1,350 (11 per cent) from foreign whistleblowers.[16] As a result of these reports, the SEC has instituted enforcement actions that have resulted in penalties of nearly US$5 billion and awarded over US$1.1 billion to 214 different whistleblowers.[17]

The Program rewards individuals for making reports pursuant to both SOX and DFA whistleblower provisions. Under both statutes, individuals qualify as whistleblowers if they report alleged misconduct and 'reasonably believe that the information [they] provide to the Commission . . . relates to a possible violation of the federal securities law'.[18] A belief is reasonable if it is both subjectively and objectively reasonable; that is, the employee must have both 'a subjectively genuine belief that the information demonstrates a possible

14 See 15 U.S.C. § 78u-6. Dodd-Frank also imposed a similar regime under the Commodity Exchange Act. See 7 U.S.C. § 26.

15 SEC, 2021 Annual Report to Congress – Whistleblower Program, 28, 31 (2021), https://www.sec.gov/files/owb-2021-annual-report.pdf.

16 Id. at 2, 38.

17 Id. at 1–2.

18 17 C.F.R. § 240.21F-2(d)(ii). Prior to 2011, the Department of Labor applied a 'definitively and specifically' standard to claims under the Sarbanes-Oxley Act [SOX], which required that the whistleblower show that the conduct was definitively and specifically related to one or more of the laws listed in SOX. See, e.g., *Welch v. Cardinal Bankshares Corp.*, ARB No. 05-064, ALJ No. 2003-SOX-15 (ARB 31 May 2007) ([w]histleblower report related to deviation from generally accepted accounting practices was not necessarily protected activity under SOX because an accounting deviation is not inherently a violation of the securities laws). However, in a 2011 decision, the Department of Labor clarified that the reasonable belief standard applied. *Sylvester v. Parexel Int'l LLC*, ARB No. 07-123, ALJ Nos. 2007-SOX-039, -042, 2011 WL 2165854, at *11 (ARB 25 May 2011). The SEC has stated that a reasonable belief is sufficient under either statute. See Implementation of the Whistleblower Provisions of Section 21f of the Sec. Exch. Act of 1934, Exchange Act Release No. 64545, 101 SEC Docket 630, 2011 WL 2045838, at *7, n. 36 (25 May 2011) [DFA Implementation Release] (adopting the reasonable belief standard and noting that the SOX anti-retaliation provision has the same requirement). However, at least some courts still apply the definitively and specifically standard for SOX claims. See, e.g., *Riddle v. First Tenn. Bank, Nat. Ass'n*, 497 F. App'x. 588, 595 (6th Cir. 2012) ('an employee's complaint must "definitively and specifically relate" to one of the six enumerated categories found in 18 U.S.C. § 1514A'). But see *Genberg v. Porter*, 882 F.3d 1249, 1255 (10th Cir. 2018) (holding that the 'definitive and specific' standard used by the district court was 'obsolete' and reversing grant of summary judgment for defendant based on that standard); *Wiest v. Lynch*, 710 F.3d 121, 131 (3d Cir. 2013) (adopting reasonable belief standard based on *Sylvester* decision).

© Law Business Research 2021

violation, and that this belief is one that a similarly situated employee might reasonably possess'.[19]

To satisfy the subjective component of this standard, the employee must have 'actually believed the conduct complained of constituted a violation of pertinent law'.[20] For the objective component, '[the] employee need not show that an actual violation occurred so long as "the employee reasonably believes that the violation is likely to happen"'.[21] 'A belief is objectively reasonable when a reasonable person with the same training and experience as the employee would believe that the conduct implicated in the employee's communication could rise to the level of a violation of' the securities laws.[22]

Although the standard for whistleblower status is similar under both statutes, there are also some material differences. First, there are differences in who is protected. SOX protects employees, contractors and subcontractors of publicly traded companies[23] and rating agencies from retaliation for reporting certain criminal offences (mail or wire fraud) or the potential violation of 'any rule or regulation of the Securities and Exchange Commission, or any provision of federal law relating to fraud against shareholders' either internally or to certain government entities.[24] The DFA, on the other hand, prohibits any

19 *Ott v. Fred Alger Mgmt., Inc.*, No. 11 Civ. 4418, 2012 WL 4767200, at *4 (S.D.N.Y. 27 Sep. 2012) (quoting DFA Implementation Release, at *7).

20 *Welch v. Chao*, 536 F.3d 269, 277 n.4 (4th Cir. 2008) (interpreting whether a plaintiff qualified for whistleblower status under SOX). See also *Ngai v. Urban Outfitters, Inc.*, No. 19-1480, 2021 WL 1175155, at *17 (E.D. Pa. 29 Mar. 2021) (finding that plaintiff did not demonstrate a subjectively reasonable belief that company had violated certain SOX provisions where his actions tended to show that he believed he was 'reporting violations of the company's own internal polices, rather than violations of federal law').

21 *Stewart v. Doral Fin. Corp.*, 997 F. Supp. 2d 129, 137 (D.P.R. 2014) (quoting *Sylvester*, 2011 WL 2165854, at *13).

22 *Wiest*, 710 F.3d at 132. See also *Yang v. Bank of New York Mellon Corp.*, No. 20-cv-3179, 2021 WL 1226661 (S.D.N.Y. 31 Mar. 2021) (interpreting whether a plaintiff demonstrated an objectively reasonable belief that company had violated SOX to qualify as a whistleblower).

23 The Supreme Court has ruled that this protection extends to employees of a non-public company who report fraud against shareholders of a public company that receives services from the non-public company. *Lawson v. FMR LLC*, 571 U.S. 429, 440 (2014). But, where the party committing the misconduct is a private company contracted by the publicly traded company and the whistleblower is an employee of the contracted company, SOX liability does not apply to the publicly traded company. *Tellez v. OTG Interactive, LLC*, No. 15 CV 8984, 2019 WL 2343202, at *4 (S.D.N.Y. 3 Jun. 2019).

24 18 U.S.C. § 1514A. Judicial decisions have made clear that disclosures regarding third parties are protected activity. See, e.g., *Sharkey v. J.P. Morgan Chase & Co.*, No. 10 Civ. 3824, 2011 WL 135026, at *5–6 (S.D.N.Y. 14 Jan. 2011) (finding that the plaintiff properly pleaded that a report concerning a third-party client's illegal activity constituted a protected activity under SOX).

© Law Business Research 2021

employer from taking adverse employment actions against employees who report potential violations of the securities laws to the SEC.[25]

Second, there are differences in the misconduct that can be reported. DFA protections only apply to whistleblowers who report potential violations of the securities laws, whereas SOX prohibits retaliation against whistleblowers who report potential violations of a wider range of laws.

Third, there are differences in the definition of retaliation. The DFA prohibits a broader range of retaliatory conduct. Pursuant to the statute, no employer 'may discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment because of any lawful act done by the whistleblower'.[26] The SOX prohibition is substantially similar, but it does not specifically prohibit indirect action against employees.[27]

Fourth, there are procedural differences in how whistleblowers must report the conduct. SOX specifically states that whistleblowers are protected against retaliation if they report misconduct internally to 'a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct)' or externally to a federal regulatory or law enforcement agency, or to the US Congress.[28] The DFA, on the other hand, statutorily defines a whistleblower as 'any individual who provides . . . information relating to a violation of the securities laws' to the SEC.[29] Recognising that SOX whistleblowers – who can report internally – are also protected under the DFA, the SEC attempted to extend DFA protection to whistleblowers who report internally pursuant to

25 The Dodd-Frank Act [DFA] defines a whistleblower as 'any individual who provides . . . information relating to a violation of the securities laws to the Commission.' 15 U.S.C. § 78u-6(a)(6).

26 15 U.S.C. § 78u-6(h)(1)(A).

27 18 U.S.C. § 1514A(a) (identified classes of employers may not 'discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the employee').

28 18 U.S.C. § 1514A(a)(1)(A)–(C). Administrative decisions have made clear that disclosures to other entities, including the Internal Revenue Service [IRS] and local law enforcement, may also be protected. See, e.g., *Vannoy v. Celanese Corp.*, ARB No. 09-118, ALJ No. 2008-SOX-064 (ARB 28 Sep. 2011) (finding that disclosures to the IRS constituted protected activity under SOX); *Funke v. Federal Express Corp.*, ARB No. 09-004, ALJ No. 2007-SOX-043 (ARB 8 Jul. 2011) (finding that reports to local law enforcement constituted protected activity).

29 15 U.S.C. § 78u-6(a)(6). This provision arguably conflicts with the broader anti-retaliation provision of the DFA, which states that an employer cannot 'discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment' in retaliation for (1) providing information to the SEC, (2) initiating, testifying in or assisting an SEC investigation or action, or (3) making disclosures that are protected by the Sarbanes-Oxley Act or 'any other law, rule, or regulation subject to the jurisdiction of' the SEC. 15 U.S.C. § 78u-6(h)(1)(A).

© Law Business Research 2021

SOX.[30] This interpretation, however, was unanimously rejected by the Supreme Court, which held that the DFA only protects employees who report misconduct to the SEC.[31]

Fifth, the statutes of limitations differ. To recover for retaliation under SOX, a whistleblower must file a complaint within 180 days of the violation.[32] The DFA, however, allows an action to be brought up to six years after the violation occurs.[33]

Finally, there are significant differences in how a whistleblower can bring a claim for retaliation. SOX is enforced by the Occupational Safety and Health Administration (OSHA), which is responsible for investigating claims.[34] Once a whistleblower makes a claim, OSHA will conduct an initial investigation to determine whether the whistleblower has made a *prima facie* showing that his or her whistleblower report was a contributing factor in an unfavourable employment decision.[35] If OSHA comes to this determination, the employer can then rebut the claim with clear and convincing evidence.[36] Once OSHA makes a final finding, either party may appeal to the Department of Labor's Office of Administrative Law Judges (ALJs).[37] The regulations then allow for limited discovery, after which an ALJ will conduct a hearing and render a decision.[38] The ALJ's decision can be appealed by the unsuccessful party to the Department of Labor's Administrative Review Board,[39] with further appeal to the United States Circuit Court of Appeals for the circuit in which the employee resided or the violation allegedly occurred.[40] Additionally, a SOX whistleblower may bring a retaliation claim in federal court if the Secretary of Labor 'has not issued a final decision within 180 days of the filing of [a] complaint and there is no showing that such delay is due to the bad faith of the claimant'.[41]

Individuals claiming DFA protections, on the other hand, may immediately bring a claim in federal court. There, courts will employ a burden-shifting standard. The employee must initially meet the 'rather light burden of showing by a preponderance of evidence that [the whistleblower report] tended to affect

30 17 C.F.R. § 240.21F-2.

31 *Digit. Realty Tr., Inc. v. Somers*, 138 S. Ct. 767 (2018).

32 18 U.S.C.A. § 1514A(b)(2)(D). See also *Xanthopoulos v. U.S. Dep't of Lab.*, 991 F.3d 823 (7th Cir. 2021) (rejecting equitable tolling of SOX claims).

33 15 U.S.C.A. § 78u-6(h)(1)(B)(iii)(I)(aa).

34 See 29 C.F.R. § 1980.104(e).

35 Id.

36 29 C.F.R. § 1980.104(e)(4).

37 29 C.F.R. § 1980.106.

38 29 C.F.R. §§ 1980.107, 1980.109.

39 29 C.F.R. § 1980.110.

40 29 C.F.R. § 1980.112.

41 18 U.S.C. § 1514A(b)(1)(B).

© Law Business Research 2021

[the adverse action] in at least some way'.[42] Once the employee has made this *prima facie* showing of retaliation, the burden shifts to the employer to prove that there was a legitimate non-retaliatory reason for the decision.[43] Only if the employer is able to provide a non-retaliatory reason does the burden shift back to the employee to show that the proffered legitimate reason is a pretext.[44]

20.1.2 The CFTC whistleblower regime

The DFA added Section 23 of the Commodity Exchange Act (CEA), which provides for whistleblower protections. The CEA anti-retaliation provision is identical to the DFA provision in the Exchange Act. Although the CEA has been used less frequently than the SEC provision by employees, given the similarities between the two, the Commodity Futures Trading Commission (CFTC) began, among other things, to strengthen its anti-retaliation protections for whistleblowers and harmonise its rules with those of the SEC's Program in May 2017. The CFTC has also explicitly stated that it will rely on SEC precedent.[45]

20.1.3 State law regimes

Many states also have laws to protect whistleblowers from retaliation but the scope of protection varies by state. For example, New York has several laws that protect whistleblowers from employer retaliation. New York's Labor Law, at Section 740, prohibits employers from taking any adverse employment action against an employee who discloses or threatens to disclose to a public body an employer's potential violation of public safety regulations, so long as the employee first brings the potential violation to the attention of their employer.[46] Healthcare workers are separately protected for reporting activities they think 'in good faith, reasonably . . . constitute[] improper quality of patient care' if they first report the perceived issue to their employer.[47] Furthermore, New York government employees are protected under New York Civil Service Law,

42 *Feldman v. L. Enf't Assocs. Corp.*, 752 F.3d 339, 348 (4th Cir. 2014).

43 DFA Implementation Release, at *8, n. 41.

44 Id.

45 See In the Matter of Claims for Award by: Redacted WB-APP Redacted; and Redacted WB-APP Redacted, in Connection with Notice of Covered Action Redacted, CFTC Whistleblower Award Determination No. 18-WB-5 (2 Aug. 2018) (The CFTC adopted principles 'consistent with those of the SEC's whistleblower program' to evaluate a whistleblower's award claim.). See also 17 C.F.R. §§ 165.15(a)(2), 165.7(f)–(1) (2017). The CFTC replaced the Whistleblower Award Determination Panel with the Claims Review Staff [CRS]. The CFTC stated that the CRS would include an enhanced review process 'similar to that established under the whistleblower rules of the US Securities and Exchange Commission'.

46 N.Y. Lab. Law § 740(2)–(3).

47 Id. § 741(2)–(3).

© Law Business Research 2021

which protects public employees who report to public health and safety officials violations that they reasonably believe to be true.[48]

The corporate perspective: preparation and response 20.2

Preparing for a whistleblower report 20.2.1

There is no legal requirement to create whistleblower policies, but companies that are potentially subject to SOX or DFA whistleblower requirements should ensure that they are prepared by creating policies and procedures that address how they will respond to and protect whistleblowers. These policies and procedures must be appropriately tailored to take into account factors such as the size of the company, the statutory whistleblower provisions that apply and the nature of its business. At a minimum, whistleblower policies should include the following three types of guidance.

First, the whistleblower policy needs to make clear how an employee or external party can report information about potential misconduct. There are a number of methods that firms can use to facilitate whistleblower reports, including designating an employee from legal or compliance who will receive those reports, creating a web-based interface for making reports or creating a telephone hotline. Ultimately, the company should adopt one or more methods that will best facilitate reports. Regardless of the method chosen, whistleblowers must also be able to escalate the report to a designated senior employee or board member in the event that the conduct implicates legal, compliance or senior executive management.

Second, the policy should explain how the company will investigate a whistleblower claim. This aspect of the policy should not mandate that specific steps will be followed in each case, as the actual nature and scope of any investigation will depend heavily on the nature and circumstances of the claim. Among the aspects that may be included are (1) who is responsible for initially investigating a whistleblower claim, (2) who is responsible for making an initial determination on the merit of the claim, (3) the circumstances under which the company will conduct a more extensive investigation, and (4) who is responsible for ultimately evaluating the whistleblower report and implementing remedial improvements if necessary.

Finally, the policy should ensure that when the identity of a whistleblower is known and the whistleblower is an employee, steps are taken to protect that person from retaliation. This protection could include designating an employee from legal or compliance to monitor the status of the whistleblower to ensure that they are not subject to adverse actions. Additionally, the policy should make clear that any personnel who retaliate against a whistleblower will be subject to discipline.

48 N.Y. Civ. Serv. § 75-b.

© Law Business Research 2021

20.2.2 Responding to a whistleblower report

Once a company learns that a whistleblower report has been made, it should adhere to its whistleblower policy. First, the company should assess the whistleblower's claim to determine what responsive action is appropriate. As discussed above, the nature of the inquiry will depend on the claim, but could range from an informal assessment by the compliance team to a formal investigation conducted by external counsel. Ultimately, the determination of how to investigate the claim will depend on the severity of the alleged conduct and the credibility of the claim. In conducting the inquiry, it is critical that the company makes clear to any employees who are interviewed that even though the substance of the interview may be protected by the company's attorney–client privilege, the employee retains the right to disclose the facts discussed during the interview to the appropriate authorities.[49]

Second, in the case of a whistleblower report by an employee whose identity is known, in addition to the steps outlined in the whistleblower policy to protect the employee, the company should also ensure that it has documented any previous warnings or disciplinary actions taken against the employee, as well as adhere to consistent disciplinary procedures. Such documentation and adherence will, if necessary, support the company's position that a whistleblower employee was disciplined or dismissed for conduct unrelated to a whistleblower report.

20.2.3 Defending anti-retaliation suits

If a whistleblower brings a retaliation action, it will be difficult, if not impossible, to defeat the action at an early stage in the litigation. This difficulty exists because the standard for what constitutes an adverse employment action is purposely vague to allow for 'a factual determination on a case-by-case basis',[50] which has been interpreted by courts to reflect a 'congressional intent to prohibit a very broad spectrum of adverse action against . . . whistleblowers'.[51] As a result, courts have refused to create a bright-line standard for what constitutes an adverse employment action and instead 'pore over each case to determine whether the challenged employment action' constitutes an adverse action.[52] While any action can be construed by an employee as retaliatory, in practice,

49 See, e.g., *In re KBR, Inc.*, Exchange Act Release No. 74619 , 111 SEC Docket 917, 2015 WL 1456619, at *2 (1 Apr. 2015) (KBR agreed to settle charges that its standard form confidentiality provision, which stated that witnesses needed permission of the company to disclose matters discussed in internal investigation interviews, undermined the Program). The company should also ensure that similar language is used in any interview conducted by counsel as part of an internal investigation.

50 DFA Implementation Release, at *8.

51 *Menendez v. Halliburton, Inc.*, ARB Nos. 09-002, -003, ALJ No. 2007-SOX-005, 2011 WL 4915750, at *10 (ARB 13 Sep. 2011) (SOX anti-retaliation claim).

52 *Wanamaker v. Columbian Rope Co.*, 108 F.3d 462, 466 (2d Cir. 1997) (ADEA anti-retaliation claim).

© Law Business Research 2021

whistleblower claims are generally predicated on conduct, such as dismissals,[53] demotions[54] or decreased compensation.[55]

Despite these difficulties, there are certain defences that may be successfully asserted in a retaliation lawsuit. First, an employer can argue that there was no causal connection between the protected activity and the adverse employment decision.[56] Two factors that can sever the causal connection are the passage of time or a legitimate intervening event. The passage of time between a whistleblower reporting and being dismissed can demonstrate that the adverse action was not retaliatory. The Second Circuit has declined to establish a bright-line rule,[57] but in the absence of additional evidence of a defendant's retaliatory motive, the passage of two months may be sufficient to sever the causal connection.[58] However, to the extent that there is evidence of other retaliatory actions against a whistleblower, courts will allow for a longer gap between the protected activity and termination.[59] Similarly, a legitimate intervening event that occurs after a whistleblower's disclosure to the SEC will sever the causal connection and create a non-retaliatory justification for dismissal. For example, one court granted summary judgment for an employer because, after making his disclosure to the SEC, the whistleblower told investors that the external directors were 'worthless', which provided a non-retaliatory justification for the whistleblower's dismissal.[60] However, because causation is generally a question of fact, a court is unlikely to decide as a matter of law that either the passage of time or an intervening event has severed the causal chain.[61]

---

53 See, e.g., *Ott*, 2012 WL 4767200, at *7 (employee alleged that she was terminated for reporting to the SEC that she believed that the hedge fund's trading policy allowed the firm to trade ahead of customer orders).

54 See, e.g., *In re Paradigm Capital Mgmt., Inc.*, Exchange Act Release No. 72393, 109 SEC Docket 430, 2014 WL 2704311 (16 Jun. 2014) (hedge fund settled claims by SEC that it retaliated against an employee who was relieved of his responsibilities following complaint).

55 See, e.g., *O'Mahony v. Accenture Ltd.*, 537 F. Supp. 2d 506, 508 (S.D.N.Y. 2008) (SOX whistleblower allegations were adequately pleaded where defendant reduced plaintiff's level of responsibility and compensation shortly after plaintiff reported defendant's alleged fraudulent activity).

56 *Fraser v. Fiduciary Tr. Co. Int'l*, No. 04 CIV. 6958, 2009 WL 2601389, at *6 (S.D.N.Y. 25 Aug. 2009) aff'd, 396 F. App'x 734 (2d Cir. 2010).

57 *Gorman-Bakos v. Cornell Coop. Extension*, 252 F.3d 545, 554 (2d Cir. 2001).

58 *Garrett v. Garden City Hotel, Inc.*, No. 05-CV-0962, 2007 WL 1174891, at *21 (E.D.N.Y. 19 Apr. 2007) (collecting cases).

59 See, e.g., *Mahony v. KeySpan Corp.*, No. 04 CV 554, 2007 WL 805813, at *6 (E.D.N.Y. 12 Mar. 2007) (denying motion for summary judgment in SOX whistleblower case despite 13-month gap between protected activity and termination because a 'reasonable juror could find that the string of retaliatory acts culminating in plaintiff's termination is evidence that plaintiff's protected activity was a contributing factor in the adverse employment action').

60 *Feldman*, 752 F.3d at 349.

61 See, e.g., *Mahony*, 2007 WL 805813, at *6 ('The gap in time between protected activity and adverse employment action is merely one factor which a jury can consider when determining

© Law Business Research 2021

An employer could argue that the whistleblower did not have a reasonable belief that the alleged conduct constituted a violation or potential violation of the securities law. In particular, whistleblower complaints need to provide more than 'self-serving averments'[62] or 'bald statement[s]'[63] in support of the claim that the plaintiff had a reasonable belief that the conduct was illegal.

There are certain defences that may be more applicable to either DFA or SOX whistleblower claims. First, DFA whistleblower claims may be amenable to arbitration. As a general principle, US federal courts 'strongly [favour] arbitration as an alternative dispute resolution process'[64] and statutory claims may be submitted to arbitration unless the statute explicitly prohibits arbitration.[65] As a result, some courts have held that DFA retaliation claims are amenable to arbitration, although a prohibition on arbitration was added to other whistleblower retaliation statutes by the DFA.[66] The Third Circuit, the only circuit court to examine this issue so far, has concluded that 'although Congress conferred on whistleblowers the right to resist the arbitration of certain types of retaliation claims, that right does not extend to Dodd-Frank claims arising under [the Dodd-Frank whistleblower provision]'.[67] SOX claims, on the other hand, are not arbitrable as a result of an amendment to SOX that was passed as part of the DFA.[68]

Finally, in some instances, an employer can argue that an anti-retaliation claim is barred because it is extraterritorial. In *Liu Meng-Lin v. Siemens AG*, for example, the Second Circuit held that DFA whistleblower protection does not generally apply extraterritorially and that the plaintiff, a resident of Taiwan who was employed by the Chinese subsidiary of a German company, did not have a valid anti-retaliation complaint because neither his report to superiors in China and Germany regarding allegedly corrupt activities that took place outside the United States, nor the decision by Siemens in Germany or China to dismiss him, had a sufficient connection to the United States to treat it as a domestic application of the statute.[69] The Second Circuit declined

---

causation. A jury may look to other facts to decide whether the protected activity precipitated the adverse employment action, including evidence of a strained relationship between the parties that portended the employee's termination.').

62 *Livingston v. Wyeth Inc.*, No. 1:03CV00919, 2006 WL 2129794, at *10 (M.D.N.C. 28 Jul. 2006).

63 *Nielsen v. AECOM Tech. Corp*, 762 F.3d 214, 223 (2d Cir. 2014).

64 *Nat'l City Golf Fin. v. Higher Ground Country Club Mgmt. Co.,* 641 F. Supp. 2d 196, 201 (S.D.N.Y. 2009).

65 *Shearson/Am. Express v. McMahon*, 482 U.S. 220, 226 (1987).

66 See, e.g., *Murray v. UBS Sec., LLC*, No. 12 Civ. 5914, 2014 WL 285093, at *11 (S.D.N.Y. 27 Jan. 2014) (holding SOX's prohibition on pre-dispute arbitration does not apply to DFA retaliation claims); *Ruhe v. Masimo Corp.*, No. SACV 11-00734, 2011 WL 4442790, at *5 (C.D. Cal. 16 Sep. 2011) (refusing to read an anti-arbitration provision into 15 U.S.C. § 78u).

67 *Khazin v. TD Ameritrade Holding Corp.*, 773 F.3d 488, 493 (3d Cir. 2014).

68 18 U.S.C. § 1514A(e)(2).

69 *Liu Meng-Lin v. Siemens AG*, 763 F.3d 175, 179–180 (2d Cir. 2014).

© Law Business Research 2021

to define the precise boundary between extraterritorial and domestic applications of the anti-retaliation provision because the case was 'extraterritorial by any reasonable definition',[70] but the Second Circuit affirmed the dismissal of foreign whistleblower claims again in *Ulrich v. Moody's Corp*, in which the alleged whistleblower was a US citizen and occasionally interacted with the company's US managers.[71] This suggests that many foreign whistleblowers may not be protected by the DFA.[72]

Anti-retaliation suits by the SEC 20.2.4

In addition to potential suits by a whistleblower, the SEC has asserted an independent right to bring whistleblower retaliation claims. In June 2014, the SEC brought its first enforcement action against a registered investment adviser for retaliation.[73] Subsequent actions show that this remains an enforcement priority for the SEC.[74] In particular, the SEC may enforce the DFA anti-retaliation provision for 'conduct occurring outside the United States that has a foreseeable substantial effect within the United States'.[75] Therefore, even if a company can successfully avoid a retaliation suit by a whistleblower on extraterritorial grounds, the SEC could still bring a suit for the same conduct.

70 *Liu Meng-Lin*, 763 F.3d at 179.

71 *Ulrich v. Moody's Corp.*, 721 Fed.Appx. 17, 19 (2d Cir. 2018) (affirming the district court's dismissal of the whistleblower complaint because 'although Ulrich, a United States citizen who sometimes interacted with Moody's United States managers, did allege more connection with the United States than was evident in *Liu*, he was nevertheless an overseas permanent resident working for a foreign subsidiary of Moody's, and the alleged wrongdoing and protected activity took place outside the United States').

72 Employers may also be able to argue that the SOX whistleblower provisions do not apply to foreign employees. See, e.g., *Asadi v. G.E. Energy (USA) LLC*, No. 4:12-345, 2012 WL 2522599 (S.D. Tex. 28 Jun. 2012) (neither SOX nor DFA anti-retaliation provisions protected US citizen employed by US company who was temporarily relocated to a foreign country because 'the majority of events giving rise to the suit occurred in a foreign country'). See also *In re Li Tao Hu*, ARB No. 2017-0068, ALJ No. 2017-SOX-00019, 2019 WL 5089597, at *6 (18 Sep. 2019) (the complaint of a foreign employee in a foreign office of a US-based company was not valid under SOX just because the retaliation decision ultimately took place in the US and the misconduct may have affected the US market). But see *Walters v. Deutsche Bank*, 2008-SOX-70, slip op. at 41 (ALJ 23 Mar. 2009) (US citizen working in Switzerland was protected as a whistleblower because 'all elements essential to establishing a prima facie violation of Section 806 allegedly occurred in the United States').

73 *In re Paradigm Capital Mgmt., Inc.*, 2014 WL 2704311.

74 See, e.g., *In re KBR, Inc.*, 2015 WL 1456619, at *3 (cease-and-desist order forbidding KBR, Inc. from violating Rule 21F-17, which prohibits companies from taking any action to impede whistleblowers from reporting possible securities violations to the SEC and imposing civil monetary penalties of US$130,000 for violations).

75 15 U.S.C. § 78aa(b)(2).

© Law Business Research 2021

20.3 The whistleblower's perspective: representing whistleblowers

In determining whether to advise a client to make a whistleblower report, there are several key preliminary considerations. First, if the client is implicated in the wrongdoing, this will affect whether they receive a whistleblower award and the amount of any award. The SEC in the DFA Implementation Release noted that 'culpable whistleblowers can enhance the Commission's ability to detect violations of the federal securities laws, increase the effectiveness and efficiency of the Commission's investigations and provide important evidence for the Commission's enforcement actions'.[76] As such, pursuant to SEC regulations, the SEC 'will assess the culpability or involvement of the whistleblower in matters associated with the Commission's action or related actions' in determining the amount of a whistleblower award.[77] In at least one case, it appears that the SEC gave an award to a culpable whistleblower. In an April 2016 order, the SEC stated that a whistleblower was subject to a parallel proceeding and that the award was 'subject to an offset for any monetary obligations', including disgorgement, prejudgment interest and penalty amounts that the whistleblower had yet to pay towards a judgment.[78] In ordering this relief, the SEC noted that the whistleblower had previously been advised of the potential offset and did not object.[79]

Second, counsel should consider whether the putative whistleblower is subject to any professional confidentiality obligations that would be implicated. In particular, SEC regulations generally exclude attorneys from recovering under the Program. Information obtained through communications that are subject to the attorney–client privilege or information obtained 'in connection with the legal representation of a client' is generally not considered 'original information'.[80] These exclusions are clearly directed at attorneys to 'send a clear, important signal to attorneys, clients, and others that there will be no prospect of financial benefit for submitting information in violation of an attorney's ethical obligations'.[81] Similarly, certain fiduciaries and professionals engaged by the company who

76 DFA Implementation Release, at *89.

77 17 C.F.R. § 240.21F-6(b)(1).

78 *In re the Claims for an Award in Connection with [Redacted]*, Exchange Act Release No. 77530, 113 SEC Docket 4529, 2016 WL 1328926, at *1 (5 Apr. 2016).

79 Id.

80 See 17 C.F.R. § 240.21F-4(b)(4)(i)–(ii).

81 See DFA Implementation Release, at *27. The SEC has provided, however, for exceptions to the attorney exclusions in order to balance an attorney's ethical obligations with the desire to prevent securities law violations. As a result, information obtained through a confidential communication or legal representation will be deemed 'original information' in three situations: (1) if the attorney is representing an issuer and reasonably believes that the disclosure is necessary to prevent the issuer from committing a material violation of the securities law or to rectify a material violation, which is likely to cause substantial injury to financial interests, or to prevent perjury or fraud upon the SEC in the course of an SEC investigation or administrative proceeding; (2) when allowed to make the disclosure pursuant to applicable state attorney conduct rules; or (3) 'otherwise'. The SEC has not

© Law Business Research 2021

obtained the information through those roles are generally not deemed to have 'original information' about misconduct.[82] However, there is no general bar on the use of information that is otherwise deemed confidential by a company.

Disclosing to the SEC 20.3.1

Neither DFA nor SOX whistleblower provisions mandate that a whistleblower make their initial disclosure to the SEC. Therefore, a whistleblower can choose to disclose initially to the SEC or first make an internal report to the employer.

From a rewards perspective, there is no benefit to disclosing first to the SEC. Pursuant to SEC regulations, the date of a whistleblower's initial internal report will be treated as the date of disclosure to the SEC, so long as the whistleblower makes a report to the SEC within 120 days of the internal report or a report to another federal agency.[83] Therefore, delaying SEC disclosure to make an internal report first will not affect whether the whistleblower is the first person to provide original information and thereby qualifies for an award.[84]

Moreover, reporting directly to the SEC could, in theory, reduce an award as one of the factors that the SEC considers in determining the amount of an award is whether the whistleblower reported the potential misconduct through internal company compliance systems and whether the whistleblower co-operated with any internal investigations.[85] Therefore, reporting directly to the SEC could reduce an award if a whistleblower is perceived to have circumvented the company's internal reporting system.

However, there is one major potential benefit to first disclosing to the SEC – guaranteed protection as a whistleblower under the DFA. In particular, the Supreme Court has held that individuals must report to the SEC in order to

provided guidance on the circumstances that would qualify an attorney to invoke the 'otherwise' exclusion.

82 17 C.F.R. § 240.21F-4(b)(4)(iii). The SEC has stated that information from these sources will not be deemed 'original' if (1) the whistleblower is in a leadership position and learned the information either from another person or in connection with internal compliance procedures, (2) the whistleblower is an internal audit or compliance employee or external adviser, (3) the whistleblower was retained to conduct an internal investigation into the company, or (4) the whistleblower is an employee of a public accounting firm, and the information was obtained while performing a function required under the federal securities laws, and relates to a violation by the client or its employees.

83 17 C.F.R. § 240.21F-4(b)(7); see also, *In re the Claim for an Award in Connection with [Redacted]*, Exchange Act Release No. 82996, 2018 WL 1693006 (5 Apr. 2018) (awarding US$2.2 million to whistleblower who initially provided notification to another federal agency).

84 See 17 C.F.R. § 240.21F-4(b) (defining 'original information' as information '[n]ot already known to the Commission from any other source').

85 See 17 C.F.R. § 240.21F-6(a)(4).

© Law Business Research 2021

be protected as whistleblowers under the DFA.[86] Therefore, if an employee only makes an internal report, the employee will lose the anti-retaliation protection provided by the DFA.[87] Moreover, because the SEC treats all whistleblower complaints as confidential and the Program provides additional confidentiality protections to ensure that a whistleblower's identity is protected, whistleblowers receive an added protection through SEC disclosure.[88]

Once a whistleblower decides to make a report to the SEC, the process itself is fairly simple. Whistleblowers may submit a complaint either through the online Tips, Complaints, and Referrals (TCR) Portal on the SEC's whistleblower website or by mailing or faxing a TCR Form to the SEC Office of the Whistleblower.[89] Once the form is received, it will be reviewed by Division of Enforcement staff, who will then determine who is best placed to investigate the allegations.[90] In some instances, the TCR will be sent to another federal or state enforcement agency, in which case information that could identify the whistleblower is generally withheld.[91]

20.3.2 Whistleblower awards under the DFA

Under the DFA, qualifying whistleblowers who provide information to the SEC leading to a successful enforcement action are entitled to an award of between 10 and 30 per cent of the funds recovered by the Commission.[92] In setting the award amount, the SEC may consider seven factors:

- the significance of information provided by the whistleblower;
- the assistance provided by the whistleblower;
- the law enforcement interest in deterring violations of securities laws;
- whistleblower participation in internal compliance systems;
- culpability;
- unreasonable reporting delay; and
- interference with internal compliance systems.[93]

---

86 *Digit. Realty*, 138 S. Ct. at 769; see also *Verble v. Morgan Stanley Smith Barney, LLC*, No. 3:14-CV-74, 2015 WL 8328561, at *5 (E.D. Tenn. 8 Dec. 2015) (employee who was dismissed for assisting federal authorities, including the FBI, was not a protected whistleblower because he had not provided information to the SEC).

87 *Digit. Realty*, 137 S. Ct. at 769.

88 17 C.F.R. § 240.21F-7. For added protection, a whistleblower may also submit a complaint anonymously through an attorney. See SEC, 2020 Annual Report to Congress – Whistleblower Program (2020), at 4, https://www.sec.gov/files/2020%20Annual%20Report_0.pdf.

89 See SEC, Office of the Whistleblower, Submit a Tip, https://www.sec.gov/about/offices/owb/owb-tips.shtml.

90 See SEC, Division of Enforcement, Enforcement Manual, at 8 (28 Nov. 2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

91 Id.

92 17 C.F.R. § 240.21F-5(b).

93 17 C.F.R. § 240.21F-6.

© Law Business Research 2021

The SEC also has the discretion to consider the potential dollar amount of the final award in its calculations.[94] In addition to the award resulting from a successful SEC action, a whistleblower whose disclosure to the SEC results in a successful action by another agency – a 'related action'[95] – may be entitled to an award of between 10 and 30 per cent of the funds collected in that action.[96] However, the SEC recently implemented a provision clarifying that a separate action may not qualify as a related action if it 'is subject to a separate monetary award program' unless the SEC determines that 'its whistleblower program has the more direct or relevant connection to the action'.[97]

Recent SEC and CFTC awards

20.3.3

The SEC awarded over US$168 million in whistleblower awards to 13 individuals in fiscal year 2018,[98] over US$60 million in whistleblower awards to eight individuals in fiscal year 2019,[99] over US$175 million to 39 individuals in fiscal year 2020[100] and over US$500 million to 108 individuals in fiscal year 2021, including the largest award ever given to an individual.[101] On 19 March 2018, the SEC awarded US$83 million to three whistleblowers in connection with

94 17 C.F.R. § 240.21F-6. But see SEC, Chair Gary Gensler, public statement, 'Statement in Connection with the SEC's Whistleblower Program' (2 Aug. 2021), https://www.sec.gov/news/public-statement/gensler-sec-whistleblower-program-2021-08-02 (announcing directive made to SEC staff to consider whether 17 C.F.R. § 240.21F-6 'should be revised . . . to clarify that the Commission will not lower an award based on its dollar amount').

95 A related action is 'a judicial or administrative action that is brought by [certain] governmental entities . . . that yields monetary sanctions, and that is based upon information that either the whistleblower [or the SEC] provided . . . to [the governmental] entity . . . and which is the same original information that the whistleblower voluntarily provided to the Commission and that led the Commission to obtain monetary sanctions totaling more than $1,000,000'. 17 C.F.R. § 240.21F-3(b)(3).

96 17 C.F.R. § 240.21F-3.

97 17 C.F.R. § 240.21F-3(b)(3)(i). But see SEC, Chair Gary Gensler, public statement, 'Statement in Connection with the SEC's Whistleblower Program' (2 Aug. 2021), https://www.sec.gov/news/public-statement/gensler-sec-whistleblower-program-2021-08-02 (announcing directive made to SEC staff to consider whether 17 C.F.R. § 240.21F-3 'should be revised to permit the Commission to make awards for related actions that might otherwise be covered by an alternative whistleblower program that is not comparable to the SEC's own program').

98 SEC, 2018 Annual Report to Congress – Whistleblower Program, at 1 (2018), https://www.sec.gov/files/sec-2018-annual-report-whistleblower-program.pdf [2018 Annual Report on Whistleblower Program].

99 SEC, 2019 Annual Report to Congress – Whistleblower Program, at 9 (2019), https://www.sec.gov/files/sec-2019-annual-report-whistleblower-program.pdf.

100 SEC, Division of Enforcement, 2020 Annual Report, at 5 (2020), https://www.sec.gov/files/enforcement-annual-report-2020.pdf.

101 Order Determining Whistleblower Award, Exchange Act Release No. 90247, File No. 2021-2 (22 Oct. 2020). See SEC, Division of Enforcement, 2021 Annual Report, at 2 (2021), https://www.sec.gov/files/owb-2021-annual-report.pdf.

© Law Business Research 2021

the SEC's US$415 million settlement with Merrill Lynch in 2016, with two whistleblowers sharing approximately US$50 million and the third receiving US$33 million for providing significant information, prompting the SEC to open two investigations and their ongoing assistance.[102] On 26 March 2019, the SEC awarded US$50 million to two whistleblowers in connection with the SEC's US$367 million settlement with JPMorgan Chase & Co in 2015, with one whistleblower receiving US$37 million – the fourth-largest award – and the other US$13 million for their information and assistance.[103] On 15 September 2021, two whistleblowers received US$114 million collectively after providing significant, independent analysis that advanced the SEC and another agency's investigations.[104]

In addition to the aforementioned trend, on 24 May 2019, the SEC granted its first award under the internal reporting provision of the Program.[105] According to the SEC, the whistleblower sent an anonymous tip-off of alleged wrongdoings to his company before submitting the same information to the SEC within 120 days. The company opened an internal investigation and reported the allegations of misconduct to the SEC, which then opened its own investigation. The company also reported the results of its internal investigation, leading the SEC to take enforcement actions. The SEC credited the whistleblower for the results of the company's internal investigation and awarded him over US$4.5 million.

The SEC has also granted whistleblower awards to individuals who have engaged in reported misconduct. On 14 September 2018, the SEC provided a financial award to a claimant, although the claimant 'unreasonably delayed in reporting information to the Commission and was culpable'.[106] Similarly,

102 SEC, press release, 'SEC Announces Its Largest-Ever Whistleblower Awards', https://www.sec.gov/news/press-release/2018-44; see also Pete Schroeder, 'U.S. SEC awards Merrill Lynch whistleblowers a record $83 million', *Reuters* (19 Mar. 2018), https://www.reuters.com/article/us-usa-sec-whistleblower/u-s-sec-awards-merrill-lynch-whistleblowers-a-record-83-million-idUSKBN1GV2MT; 2018 Annual Report on Whistleblower Program, supra note 98, at 10.

103 SEC, press release, 'SEC Awards $50 Million to Two Whistleblowers', https://www.sec.gov/news/press-release/2019-42; see also Matt Robinson and Neil Weinberg, 'Whistleblowers Awarded $50 Million by SEC in JPMorgan Case', *Bloomberg* (26 Mar. 2019), https://www.bloomberg.com/news/articles/2019-03-26/two-whistleblowers-awarded-50-million-for-aiding-sec-case.

104 Order Determining Whistleblower Award, Exchange Act Release No. 90247 (22 Oct. 2020).

105 SEC, press release, 'SEC Awards $4.5 Million to Whistleblower Whose Internal Reporting Led to Successful SEC Case and Related Action', https://www.sec.gov/news/press-release/2019-76.

106 *In re the Claim for Award in Connection with [Redacted]*, Exchange Act Release No. 84125, 2018 WL 4382861, at *1 (14 Sep. 2018).

© Law Business Research 2021

on 26 March 2019, the SEC awarded a whistleblower (Claimant #1) an unreported sum despite Claimant #1's participation in the reported misconduct.[107]

The CFTC has also shown an upward trend in granting whistleblower awards in increasing amounts. Starting with its first award of US$246,000 on 20 May 2014, the CFTC issued one award for US$300,000 in 2015, two awards totalling US$11,551,320 in 2016, five awards totalling US$75,575,113 in 2018 and five awards totalling approximately US$15 million in fiscal year 2019.[108] Similarly, the CFTC's whistleblower programme has seen significant advancement and growth.

Three notable CFTC whistleblower awards to date took place in 2018. On 12 July 2018, the CFTC granted approximately US$30 million to a whistleblower who provided key information relating to the 2015 settlement with JPMorgan Chase & Co, which also settled with the SEC.[109] On 16 July 2018, the CFTC gave an award to a foreign whistleblower for the first time, providing over US$70,000 for significant contributions to the CFTC investigation and demonstrating the international reach of the whistleblower programme through an online system.[110] On 2 August 2018, the CFTC granted multiple whistleblower awards totalling more than US$45 million, and the Director of the CFTC's Division of Enforcement announced that he expected the trend to continue.[111] Although the awards in fiscal year 2020 were not as large as those handed down in 2018, the CFTC awarded close to US$20 million to whistleblowers in 2020 and released its largest award yet in 2021 with a US$200 million award to a whistleblower whose specific, credible information contributed to an open investigation and led to three successful enforcement actions.[112]

---

107 *In re the Claims for Award in Connection with [Redacted]*, Exchange Act Release No. 85412, 2019 WL 1353776, at *2 (26 Mar. 2019). Claimant #1's reward was reduced because Claimant #1 delayed reporting and continued to passively benefit financially from the 'underlying misconduct during a portion of the period of delay'.

108 US Commodity Futures Trading Commission [CFTC], Annual Report on the Whistleblower Program and Customer Education Initiatives (Oct. 2019), https://whistleblower.gov/sites/whistleblower/files/2019-10/FY19%20Annual%20Whistleblower%20Report%20to%20Congress%20Final.pdf.

109 CFTC, press release, 'CFTC Announces Its Largest Ever Whistleblower Award of Approximately $30 Million', https://www.cftc.gov/PressRoom/PressReleases/7753-18; Henry Cutter, 'JPMorgan Whistleblower Set to Get Largest Payout from CFTC', *Wall St. J.* (12 Jul. 2018), https://www.wsj.com/articles/jpmorgan-whistleblower-set-to-get-largest-payout-from-cftc-1531421603?mod=djemRiskCompliance&ns=prod/accounts-wsj.

110 CFTC, press release, 'CFTC Announces First Whistleblower Award to a Foreign Whistleblower', https://www.cftc.gov/PressRoom/PressReleases/7755-18.

111 CFTC, press release, 'CFTC Announces Multiple Whistleblower Awards Totaling More than $45 Million', https://www.cftc.gov/PressRoom/PressReleases/7767-18.

112 CFTC, press release, 'CFTC Awards Nearly $200 Million to a Whistleblower', https://www.cftc.gov/PressRoom/PressReleases/8453-21.

© Law Business Research 2021

20.4 Filing a qui tam action under the False Claims Act

Individuals who report fraud against the United States government have another option for disclosing information – the False Claims Act. This Act was created in 1863 initially to combat price-gouging during the Civil War but the modern incarnation of the statute is a result of congressional concern regarding defence procurement fraud.[113] Since the statute was enhanced in 1986, there has been a significant growth in False Claims Act suits, from 30 in 1987 to 633 in 2019.[114] As a result of these suits, the US Department of Justice (DOJ) collected US$62 billion between 1986 and 2019, including over US$3 billion in fiscal year 2019 alone.[115]

The False Claims Act can be used to prosecute claims for false monetary claims against the government, false statements in aid of false claims, conspiracies to defraud the government into paying a false claim, or false statements intended to reduce an obligation to the government.[116] Moreover, pursuant to the False Claims Act, private individuals – referred to as relators – may bring *qui tam* claims on behalf of the government alleging that a defendant has committed fraud against the US government.[117] If the prosecution of the *qui tam* claim is successful, the relator may receive between 15 per cent and 30 per cent of the recovery.[118] This can result in substantial compensation for a whistleblower, as False Claims Act defendants may be liable for penalties of US$5,000 to US$10,000 per violation and for treble damages.[119]

20.4.1 How a qui tam action operates

To bring a *qui tam* action, the relator must file their complaint in federal court under seal.[120] The initial complaint is only served on the DOJ, which has 60 days to examine the merits of the claim.[121] During this 60-day period (which is often extended), the DOJ will determine whether to terminate or settle the

113 *United States ex rel. Springfield Terminal Ry. Co. v. Quinn*, 14 F.3d 645, 649-51 (D.C. Cir. 1994). Defence contracting remains one of the most frequent targets of *qui tam* complaints, constituting approximately 14 per cent of *qui tam* complaints. The healthcare industry is the most frequent target, accounting for approximately 58 per cent of *qui tam* complaints. US Dep't of Justice [DOJ], Fraud Statistics – Overview: 1 October 1986 – 30 September 2017 (19 Dec. 2017), https://www.justice.gov/opa/press-release/file/1020126/download.

114 DOJ, press release, 'Justice Department Recovers over $3 Billion from False Claims Act Cases in Fiscal Year 2019', https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019.

115 Id.

116 31 U.S.C. § 3729.

117 31 U.S.C. § 3730(b).

118 See 31 U.S.C. § 3730(d). However, as discussed further below, this can in some circumstances be reduced to 10 per cent or less. See infra notes 122 to 129 and accompanying text.

119 31 U.S.C. § 3729(a)(1).

120 31 U.S.C. § 3730(b).

121 Id.

© Law Business Research 2021

claim, intervene and take 'primary responsibility' for the claim, or decline to intervene and allow the relator to proceed alone.[122] After this period expires, the complaint is unsealed and the defendant will receive notice of the claim.

At this stage, the government's 'ultimate election among the options has a direct effect on the relator's right to share in a recovery'.[123] If the government decides to intervene in the action, the relator is entitled to 15 per cent to 25 per cent of any recovery, while the government receives the remaining recovery.[124] The precise amount will 'depend[] upon the extent to which the person substantially contributed to the prosecution of the action'.[125] If, on the other hand, the government decides not to pursue the case, the relator will be entitled to 25 per cent to 30 per cent of the recovery, with the government again receiving the remainder of the recovery. The relator is also entitled to 'an amount for reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs'.[126] However, one study has revealed that the majority of plaintiffs voluntarily dismiss the *qui tam* action if the DOJ declines to intervene,[127] despite the potential for a larger award.

In addition to this basic framework, there are also limitations on awards, which may reduce or eliminate a possible award. First, a relator's award will be reduced if they 'planned and initiated' the False Claims Act violation.[128] Second, if the court determines that the information is 'based primarily on disclosures of specific information' relating to government investigations or news accounts, the award will be reduced to no more 'than 10 percent of the proceeds, taking into account the significance of the information and the role of the person bringing the action in advancing the case to litigation'.[129] Finally, a relator is entitled to no award if they are 'convicted of criminal conduct arising from his or her role in the violation'.[130] Additionally, there are provisions that preclude filing additional suits based on substantially similar *qui tam* or government enforcement proceedings.[131] These provisions are intended to achieve 'the golden mean between adequate incentives for whistle-blowing insiders . . . and

122 31 U.S.C. § 3730(b)–(c).

123 *Roberts v. Accenture*, LLP, 707 F.3d 1011, 1015 (8th Cir. 2013).

124 31 U.S.C. § 3730(d)(1).

125 Id.

126 Id.

127 See David Freeman Engstrom, 'Public Regulation of Private Enforcement: Empirical Analysis of DOJ Oversight of Qui Tam Litigation Under the False Claims Act', 107 *Nw. U. L. Rev.* 1717, 1718 (stating that in a randomly selected 460 case subsamples of the 4,000 unsealed *qui tam* actions filed between 1986 and 2011 'roughly 60% of cases in which DOJ declined intervention appeared to generate no further litigation prior to a voluntary dismissal by the relator').

128 31 U.S.C. § 3730(d)(3).

129 31 U.S.C. § 3730(d)(1).

130 31 U.S.C. § 3730(d)(3).

131 31 U.S.C. § 3730(e)(4)(A).

© Law Business Research 2021

discouragement of opportunistic plaintiffs who have no significant information to contribute of their own'.[132]

In addition to determining the quantum of a *qui tam* award, the DOJ's decision may also have a substantial impact on the outcome of the lawsuit. Statistics published by the DOJ show that cases where the DOJ intervenes are substantially more likely to generate recoveries than declined cases.[133] DOJ declination may also signal a lack of merit to the court.[134]

DOJ policy enacted in 2020 also encourages DOJ attorneys to 'consider whether the government's interests are served' by seeking dismissal of the *qui tam* action.[135] Pursuant to this policy, DOJ attorneys are encouraged to seek dismissal to:

- curb meritless *qui tam* actions;
- prevent 'parasitic or opportunistic' actions that duplicate a pre-existing investigation;
- prevent interference with government programmes;
- preserve the DOJ's litigation prerogatives;
- safeguard national security;
- preserve government resources; or
- address 'egregious procedural errors' that would frustrate a proper investigation.[136]

However, even if the DOJ decides not to intervene a case, it still has an oversight role in the litigation. First, the DOJ retains the continuing right to dismiss

132 *Springfield Terminal Ry. Co.*, 14 F.3d, at 649.

133 See DOJ, Fraud Statistics – Overview: 1 October 1987 – 30 September 2015 (12 Jul. 2016), https://www.justice.gov/civil/file/874921/download (indicating that settlements and judgments in qui tam actions where the government intervened represented 94 per cent of all *qui tam* settlements and judgments obtained between 1987 and 2015).

134 See, e.g., *United States ex rel. Jamison v. McKesson Corp.*, 649 F.3d 322, 331 (5th Cir. 2011) (noting that DOJ decision to intervene in cases involving seven of 400 defendants suggested that the unintervened claims 'presumably lacked merit'); *United States ex rel. Karvelas v. Melrose-Wakefield Hosp.*, 360 F.3d 220, 242 n. 31 (1st Cir. 2004) ('the government's decision not to intervene in the action also suggested that [relator's] pleadings of fraud were potentially inadequate'); *United States ex rel. Mikes v. Straus*, 78 F. Supp. 2d 223, 225–26 (S.D.N.Y. 1999) (suggesting that 'the reason the Government chose not to intervene in this matter is its recognition that Relator's allegations . . . were a "stretch" under the False Claims Act'). But see *United States ex rel. Williams v. Bell Helicopter Textron Inc.*, 417 F.3d 450, 455 (5th Cir. 2005) (noting that 'a decision not to intervene may not [necessarily be] an admission by the United States that it has suffered no injury in fact, but rather [the result of] a cost-benefit analysis' (citations and internal quotation marks omitted)); *United States ex rel. Downy v. Corning*, Inc., 118 F. Supp. 2d 1160, 1170 (D.N.M. 2000) (noting that intervention decision may have been driven by 'lack of available Assistant United States Attorneys or respect for the skill of the relator's attorneys').

135 DOJ, Justice Manual § 4-4.111 (2020).

136 Id.

© Law Business Research 2021

or settle an action being prosecuted by a relator,[137] although at least some courts have suggested that this is not an absolute right.[138] Second, the DOJ retains the right to veto private dismissals or settlements because any judgment will have preclusive effect on a future lawsuit by the US government based on the same facts.[139] That said, a minority of courts have held that the DOJ can only object by showing 'good cause' in a case where it has not intervened.[140]

Effects of filing a qui tam action 20.4.2

A *qui tam* action can have a substantial impact on both the relator and the defendant. First, the relator faces both reputational and financial risk. By filing a *qui tam* action the relator has agreed to be publicly identified because the unsealed complaint will identify the relator as the complainant.[141] Relators have tried to avoid this consequence by moving to dismiss and seal cases if the DOJ declines to intervene but have met with, at best, limited success.[142] For relators who are still employed by the defendant, this risk is mitigated by the anti-retaliation provisions in the False Claims Act, which provide for reinstatement and double damages in the event of retaliation.[143] Nonetheless, depending on the situation, relators may have legitimate concerns about the impact on their professional reputations.

137 31 U.S.C. § 3730(c)(2)(b).

138 See *United States ex rel. Sequoia Orange Co. v. Baird-Neece Packing Corp.*, 151 F.3d 1139, 1145 (9th Cir. 1998) ('[a] two step analysis applies here to test the justification for dismissal: (1) identification of a valid government purpose; and (2) a rational relation between dismissal and accomplishment of the purpose' (internal citations and quotation marks omitted).

139 See, e.g., *Searcy v. Philips Elecs. N. Am. Corp.*, 117 F.3d 154, 160 (5th Cir. 1997) (noting the 'danger that a relator can boost the value of settlement by bargaining away claims on behalf of the United States').

140 *United States ex rel. Killingsworth v. Northrop Corp.*, 25 F.3d 715, 722 (9th Cir. 1994); but see *Ridenour v. Kaiser-Hill Co.*, 397 F.3d 925, 931 n. 8 (10th Cir. 2005) ('[e]ven where the Government has declined to intervene, relators are required to obtain government approval prior to entering a settlement or voluntarily dismissing the action')

141 *United States ex rel. Wenzel v. Pfizer, Inc.*, 881 F. Supp. 2d 217, 222–23 (D. Mass. 2012) ('[relator] filed his claim with the expectation that his identity would be revealed to the public in the event that the government entered the case'). Relators have attempted to avoid this outcome by filing under a pseudonym or creating a corporation to file the complaint. This strategy, however, will only work if the case is not litigated. If it is litigated, this is unlikely to provide significant protection because the defendant is likely to seek discovery regarding the relator's identity and the basis of their knowledge. Moreover, in some cases there is no way to effectively hide the source of the information. See, e.g., *US ex rel. Permison v. Superlative Technologies, Inc.* 492 F.Supp.2d 561, 565 (E.D. Va. 2007) (noting that 'it is doubtful that redaction would provide any protection given the very specific allegations contained in the complaint').

142 881 F. Supp. 2d., at 221 (collecting cases and noting that '[m]ost courts have . . . decided that a relator's general fear of retaliation is insufficient to rebut the presumption of public access').

143 31 U.S.C. § 3730(h).

© Law Business Research 2021

Relators often face additional financial risks if the government declines to intervene. In particular, relators may be responsible for the defendant's reasonable legal fees if the defendant prevails and 'the court finds that the claim of the person bringing the action was clearly frivolous, clearly vexatious, or brought primarily for purposes of harassment'.[144]

A *qui tam* action also creates financial and reputational risks for a defendant. A successful *qui tam* action could cost a corporation millions, if not billions, of dollars.[145] Moreover, defendants also risk debarment from additional federal contracts.[146] From a reputational perspective, the corporation faces negative publicity associated with public accusations of committing fraud against the government, although at least one court has suggested that this impact is minimised when the DOJ declines to intervene.[147]

144 31 U.S.C. § 3730(d)(4). US courts also have the inherent authority to impose sanctions, as well as authority pursuant to Rule 11 of the Federal Rules of Civil Procedure.

145 See, e.g., DOJ, press release, 'GlaxoSmithKline to Plead Guilty and Pay $3 Billion to Resolve Fraud Allegations and Failure to Report Safety Data', https://www.justice.gov/opa/pr/glaxosmithkline-plead-guilty-and-pay-3-billion-resolve-fraud-allegations-and-failure-report (announcing settlement of civil and criminal actions against pharmaceutical company, including a US$1.043 billion settlement resolving four related *qui tam* actions).

146 48 C.F.R. 9.406-2 (2021).

147 *United States ex rel. Pilon v. Martin Marietta Corp.*, 60 F.3d 995, 999 (2d Cir. 1995) ('a defendant's reputation is protected to some degree when a meritless qui tam action is filed, because the public will know that the government had an opportunity to review the claims but elected not to pursue them').

© Law Business Research 2021

21

Whistleblowers: The In-house Perspective

Steve Young[1]

Initial considerations 21.1

Most whistleblowing policies provide several channels for staff to raise concerns. These often include the staff member's line manager (or a more senior manager), human resources, audit, legal, compliance or dedicated ethics, or integrity, departments.

The desired culture of any corporate must be that staff feel entirely comfortable raising concerns with their immediate line manager, who in turn will escalate the issue to the appropriate department. Should whistleblowers prefer not to go to their line manager, they should feel able to approach someone in the organisation they trust. The culture corporates should aspire to must be one where employees may raise concerns with the full confidence they will be treated with respect, will be taken seriously and will suffer no retaliation in any form.

From an in-house perspective, it is always an initial concern that an employee has not had sufficient confidence in the organisation to raise the matter via internal personnel in the normal course of business. Resorting to the whistleblowing channels sends a message itself, and more so if the employee has chosen to remain anonymous. Monitoring and analysing whistleblowing cases can provide a measure of the organisation's culture and confidence levels for raising concerns. While much depends on the nature of the concern, the tone from the top and creating a culture that speaking up is the right thing to do are imperative. Many organisations now include questions in employee opinion surveys to try to gauge the level of confidence staff have in raising their concerns. Some other initial considerations are pointed out below.

1 Steve Young is the CEO of the Association of Corporate Investigators and head of fraud and investigations at Banque Lombard Odier & Co Ltd.

© Law Business Research 2021

- *Culture*: Creating a culture in which staff have confidence to raise concerns internally is becoming increasingly important as some regulatory authorities now mandate regulated firms to include regulatory whistleblowing hotline numbers and email addresses in corporate whistleblowing policies, for example at UK branches of overseas banks.[2] Additionally, proposals to extend the scope of whistleblower awards, for example the US Securities and Exchange Commission's proposal to allow awards based on information from a whistleblower that leads to deferred prosecution agreements and non-prosecution agreements entered into by the US Department of Justice,[3] if adopted, raises the possibility of direct reporting to regulators bypassing internal reporting channels.
- *Anonymity*: Anonymous whistleblowers can deny the investigator the opportunity to open a constructive dialogue to seek further information, put matters into context and limit feedback. A key challenge for the investigator is why the whistleblower wished to remain anonymous. It can be helpful to simply ask the question if there is a communication channel, such as webmail, open with the whistleblower.
- *The nature of the allegation and motive for reporting*: While investigators should always keep an open mind, the motive of the whistleblower often becomes apparent as the facts are established. If a dialogue with the whistleblower exists, they can be asked their motive for reporting.
- *Duration*: How long the alleged conduct has been taking place is material. Aged issues can present problems such as records retention periods. In addition, because of staff turnover, accessibility to ex-employees can be a problem.
- *Existing knowledge from another source*: Investigators should check corporate records, such as audit, risk, legal and compliance, to check if the alleged activity is known and was previously or is currently the subject of investigation.
- *Need for external counsel*: Investigators should lean towards caution during the initial review of a whistleblower allegation and take legal advice at an early stage. Assessment of the legal risks by an internal or external lawyer will prevent problems arising later if the investigation uncovers serious wrongdoing.
- *The welfare of the whistleblower and duty of care*: Investigators should keep in mind the welfare of the whistleblower. For most it will not have been an easy decision to speak up. Stay mindful of health and performance impacts – and the legal risk of these to the organisation.

2 See https://www.fca.org.uk/publication/policy/ps17-07.pdf.

3 See https://www.sec.gov/news/press-release/2018-120.

© Law Business Research 2021

- *Protecting the whistleblower from retaliation*: In the event that a whistleblower is identified, immediate steps may need to be considered to prevent retaliation. These could include moving the whistleblower to another part of the organisation, or transferring to an alternative line manager. Much depends on the nature of the case.

Identifying legitimate whistleblower claims 21.2

Given the wide range of concerns raised by whistleblowers, distinguishing between legitimate and non-legitimate allegations should be dictated by the facts gathered during the investigation. In some cases, a prompt review of the matters alleged by a subject-matter expert can quickly point to whether something is 'off-target' or requires further investigation. During the normal course of document examination, email reviews, staff interviews and data analysis generally the allegations can be substantiated or disproved. While some allegations will always be inconclusive, more frequently in human resources cases, generally a determination can be reached on the facts. Whistleblowing cases that contain multiple allegations require a detailed breakdown of each allegation as some parts may prove substantive while others will be off-target. Whistleblowing allegations are never suited to a one-size-fits-all approach and much depends on the nature of each case.

On receipt of a whistleblowing allegation, first steps should include checks to ascertain if the matters raised are known or the subject of an ongoing or previous investigation.

Generally, allegations can be split into three categories:

- material allegations that expose the corporate to regulatory action, civil claims or criminal investigation. These require experienced legal advice and depending on the jurisdiction investigation by external counsel to preserve privilege and advise the corporate accordingly;
- allegations of wrongdoing, including internal fraud and breaches of the code of conduct or policies and procedures. These generally can be investigated by internal corporate investigators, or external forensic firms with internal or external legal advice and oversight if required; and
- behavioural allegations such as bullying, harassment, inappropriate relationships, etc., which can generally be investigated by human resources or independent line management. Allegations of a sexual nature may require specialist investigative expertise. The nature of these allegations should be reviewed to consider who is best suited to undertake the investigation. The #MeToo movement has seen an increase in sexual allegations that may require specialist investigative, legal and victim care management.

Employee approaches to whistleblowers 21.3

A key component of any corporate whistleblowing policy must include a zero-tolerance approach to any retaliation against a whistleblower. Retaliation or perceived retaliation against a whistleblower raises cultural and legal risk, and undermines the effectiveness of a whistleblowing programme. Frequently

© Law Business Research 2021

during whistleblowing investigations, especially ones involving allegations of wrongdoing by senior management, interviewees speculate as to who the whistleblower might be. Ideally, in the absence of a legal obligation to do so (e.g., in litigation or in some jurisdictions) it is preferable that there is no such disclosure.

Speculation among staff should be discouraged, as it can increase the risk of retaliation.

Retaliation against whistleblowers can take many forms; examples include silence, isolation, inappropriate remarks, threats and work sabotage. In the event that a staff member or number of staff members are acting inappropriately towards a whistleblower, action will need to be taken.

Good investigation process separates the collection of facts and evidence gathering from decision-making to determine outcomes. This is particularly important when an investigator is putting forward information concerning retaliation against a whistleblower. As a general rule the investigator should not be involved in the sanctions or enforcement actions against retaliators – it is a separate legal and HR issue.

If the whistleblower's identity is known, dialogue should take place about the treatment the whistleblower is receiving and whether he or she has disclosed to anyone that they have raised the matter. Special care is required if the retaliation is by a line manager. The whistleblower should be given an opportunity to express his or her expectations and view as to what could be done. Investigators should be mindful that the organisation will generally have a duty of care and the whistleblower could take action against the organisation in the future.

Frequently whistleblowers experiencing retaliation or those believing they are being treated differently suffer health problems, such as stress leading to time off work. In these circumstances, referrals via human resources to confidential staff welfare support schemes should be considered. In determining the action to be taken against staff involved in retaliation against a whistleblower, the investigator should consult with human resources, legal, compliance and business management functions for the next steps, which could include disciplinary action up to and including dismissal.

Appropriate action taken against those who retaliate against whistleblowers can send a strong message to reinforce the culture of the organisation.

21.4 Distinctive aspects of investigations involving whistleblowers

Corporates with in-house investigation departments generally have investigation procedures in place that also apply to whistleblowing cases. The substantive difference is how the matter was raised. Investigators should proceed with the protection of the whistleblower as a top priority. Thought should be given to lines of enquiry or staff interviews that could identify the whistleblower. The general rule to note is that it is the matter under investigation that is the issue, not how the matter came to the organisation's attention.

Investigators should check if local law requires disclosure that the matter was raised as the result of a whistleblower. It is generally not a requirement in

© Law Business Research 2021

law to disclose to those facing allegations that the matter under investigation was raised by a whistleblower.

A good example of an exception is France, where it is generally required that accused persons be informed of whistleblowing allegations made against them so they may respond to them. They also have protection against malicious allegations. In this respect investigators should be mindful that, in the rare cases of malicious allegations, the alleged party, or the employer, may consider legal action against an identifiable whistleblower.

Equally, as with many investigations, consideration must be given to the collection and recording of personal data. Legal advice should be taken on data protection obligations, as again, in some jurisdictions such as France, an accused person may be informed of the accusation and have a right of challenge when his or her personal data is recorded during a whistleblowing investigation.

With the protection of the whistleblower and disclosure obligations at the top of the investigator's priority list, it is important the internal investigation proceeds as with any other investigation to establish the facts. Establishing a dialogue with the whistleblower, if possible, allows for further information, context and feedback to take place. It can be that allegations are raised in good faith but are off-target owing to facts unknown to the whistleblower.

In the event the allegation, or allegations, are substantiated and lead to regulatory enforcement action, litigation by way of civil claims or criminal investigation, or all three, it may be that the identity of the whistleblower, if known, must be disclosed. Investigators should be mindful not to give whistleblowers definitive commitments of non-disclosure, even if authorities have whistleblower protections in place. In serious cases, this aspect requires early legal advice when the allegation is first received and assessed, as the legal risks will require consideration.

Everyone involved in the whistleblowing investigation and management process should remain aware that whistleblowers are free to speak to whomever they wish and this can include law enforcement, external regulators and taking their own external legal advice. Specialist legal advice should be taken in respect of employees who have raised concerns where the employer is considering reaching a settlement involving a non-disclosure agreement. Some jurisdictions consider these counterproductive to the aims of whistleblowing programmes. In the United Kingdom, the All Party Parliamentary Group on Whistleblowing[4] has called for legislation to ban the use of non-disclosure agreements for whistleblowers.

The covid-19 pandemic and whistleblowing 21.5

The pandemic has seen a significant increase in whistleblowing cases reported in the public and private health sector. In addition to health, since March 2020, regulators have been receiving an increased number of fraud and

4 https://www.appgwhistleblowing.co.uk/.

© Law Business Research 2021

financial misstatement whistleblowing reports. This trend is likely to continue as the economic downturn takes hold. Whistleblowing reports traditionally rise in times of economic stress, and this pandemic has brought new challenges. The imposition of public health protection measures across the world has seen unprecedented numbers of employees working remotely from home. From an in-house perspective this has resulted in whistleblowing investigations being conducted remotely because of enforced travel bans and respect for social distancing. Organisations should ensure all whistleblowing channels are working effectively. In-house procedures should remain unchanged and protection protocols reinforced to ensure employees working remotely and potentially feeling isolated from colleagues are confident that organisations continue to take whistleblowing seriously and they are protected from retaliation. From a practical perspective, in-house investigators, lawyers and external counsel have become well versed in remote interviewing and investigating using audio and videoconferencing. Equally, many employees have now adapted to video meetings and conferences. While these technologies were widely used by many organisations the pandemic has brought about a new normal in remote working, which is expected to continue. Whistleblowing professionals will equally need to adapt. Ensuring confidentially can be maintained with an audio or video meeting with a whistleblower will require investigation procedures to be amended to cover security. If they are to be recorded, appropriate legal advice on privilege and consent should be obtained. Aside from the challenges of working remotely, such as building a rapport and maintaining regular contact with the whistleblower for feedback and welfare, the whistleblowing investigation process should proceed as normal.

21.6 The European Union Whistleblower Directive

Directive (EU) 2019/1937[5] requires Member States to implement legislation (by 17 December 2021) to protect whistleblowers who report violations of EU law. Member States will decide if their transposition of the directive covers breaches of national law as well as EU law, and they may extend national legislation to encompass a broader scope or stricter standards. The directive should be viewed as providing the minimum standards. Practitioners conducting investigations in member states in organisations with 50 or more workers should check the local legislation for regulation on protecting the confidentiality of whistleblowers and the investigation.[6] The requirements to promptly acknowledge receipt of reports and provide timely feedback should also be

5 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937.

6 Following its departure from the European Union, the United Kingdom is not required to implement the Whistleblower Directive. Despite Protect, the whistleblowing charity, urging the UK government to bring the new provisions into domestic law, there are no proposals to do so.

© Law Business Research 2021

clearly understood. As the directive seeks to increase protection for whistleblowers, those responsible for investigating whistleblower reports should be wary of lines of enquiry that could identify whistleblowers and leave them open to retaliation. The directive includes no obligation to respond to or investigate reports from anonymous sources; however, generally in-house practitioners are encouraged to look at the nature of the allegation rather than how it was communicated. Following up with whistleblowers who make anonymous reports without compromising anonymity is easily achieved.

International Standards Organisation whistleblowing management systems 21.7

In July 2021, the International Standards Organisation (ISO) published ISO 37002, Whistleblowing management systems – Guidelines.[7] The standards provide guidance for managing the whistleblowing process end to end. Many in-house whistleblowing management practitioners will find the standards useful guidance. For organisations in regulated sectors, compliance with the standards will assist meeting regulatory expectations. From the in-house investigations' perspective, the guidance points to specific standards for managing whistleblowing investigations that will be useful.

The guidelines define a whistleblowing investigation as a systemic, independent and documented process for establishing facts and evaluating them objectively to determine if wrongdoing has occurred, is occurring or is likely to occur, and its extent. An investigation can be an internal investigation conducted by the organisation or by an external party on its behalf. It can be a combined investigation.

The guidance outlines principles for the management of whistleblowing investigations which include, but are not limited to, the following:

- Investigations should be adequately resourced.
- Clear terms of reference and scope should be defined and documented.
- The investigation process should be robust enough to withstand administrative, operational and legal review. An audit trail should be maintained relating investigation activities back to approved plans. The investigation should consider any subject of a report as being presumed innocent.
- The investigation should not directly or indirectly interfere with a judicial investigation. It should cooperate where appropriate or required.
- The investigation should secure and protect evidence.
- The personal data should be managed in line with data privacy and protection, law and regulation.
- The investigation should protect any information that could identify any subject of a report.
- All investigations should be able to scale and adapt as the circumstances can change as the investigation progresses.

7 https://www.iso.org/standard/65035.html.

© Law Business Research 2021

- Communication should be clear and unambiguous, balancing the interests of organisations and whistleblowers.
- Organisations should communicate regularly, including material progress, in the form of feedback to the whistleblower.

On the protection of whistleblowers, the guidance recommends conducting investigations in a manner that preserves confidentiality to the extent possible and appropriate to ensure the subjects are not exposed to reputational harm, with information shared on a strictly need-to-know basis.

In-house whistleblowing investigation practitioners will welcome the ISO whistleblowing guidelines as a useful addition to the growing library of best practice resources available on this topic.

© Law Business Research 2021

22

Forensic Accounting Skills in Investigations

Glenn Pomerantz and Daniel Burget[1]

Introduction 22.1

The purpose of this chapter is to explain key steps and best practices in investigations from an accounting perspective. The term 'forensic', as defined in Webster's Dictionary, means 'belonging to, used in or suitable to courts of judicature or to public discussion and debate'. Accordingly, forensic accounting involves the application of specialised knowledge and investigative skills to matters in anticipation of possible litigation or dispute resolution, including in civil, administrative or criminal enforcement matters. Forensic accounting skills can be applied to a wide variety of investigations into alleged corporate and individual wrongdoing, including:

- misappropriation of assets by employees;
- bribery and corruption;
- money laundering;
- financial reporting fraud;
- non-compliance with laws, regulations or provisions of contracts; and
- fraud perpetrated by vendors or suppliers and other third parties.

We may refer to non-compliance instead of fraud. Non-compliance often lacks the intent of fraud and may manifest itself in the violation of an agreement, policy or otherwise acceptable behaviour. Investigations may focus on allegations of fraud or non-compliance.

The range of specialisations within the field of forensic accounting is diverse, but at the core is a focus on accounting systems, processes, records, data

1 Glenn Pomerantz is a partner and Daniel Burget is a director at BDO USA, LLP.

© Law Business Research 2021

and reports. A logical order in which forensic accountants will proceed in an investigation is as follows:

- gaining a broad understanding of allegations, accounting systems, employee responsibilities and business processes;
- preserving records and other evidence;
- mitigating losses;
- developing a workplan for the investigation;
- considering and carrying out data analytics, email review (often with counsel) and review of books and records;
- conducting (often with counsel) information-gathering interviews; and
- conducting (often with counsel) investigative interviews.

Many of the most important steps involved in this process are explained in this chapter.

22.2 Regulator expectations

In June 2020, the US Department of Justice (DOJ) set forth additional guidance[2] on how it evaluates corporate compliance programmes for assessment and sentencing purposes. Forensic accountants are well suited to help to develop effective compliance programmes or evaluate the efficacy of an existing programme. The DOJ guidance represents an authoritative road map for the building or enhancement of a programme, and adds detail and emphasis to the April 2019 guidance.[3] It remains centred on three primary questions: (1) Is the programme well designed? (2) Is the programme adequately resourced and empowered to function effectively? (3) Does the programme work in practice?

The context of the DOJ's guidance is to assist prosecutors to evaluate a corporation's compliance programme in determining the form of any resolution or prosecution, monetary penalties and further compliance obligations such as a monitorship. Corporations, however, may use the guidance as a resource for building or enhancing their compliance programme. The DOJ guidance challenges the compliance professional with several hundred questions related to their existing programme. Although forensic accounting professionals collaborate with attorneys, auditors and several types of consultants to assist in-house compliance professionals with practically all aspects of their compliance programme, the DOJ's revised guidance addresses the following key factors most applicable to forensic accounting:

- risk assessments and in particular fraud risk assessments;
- internal control testing
- risk metrics including analytics;

2 U.S. Dep't of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020).

3 U.S. Dep't of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Updated April 2019).

© Law Business Research 2021

- gatekeeper training on the control processes;
- third-party management;
- internal audit and compliance function autonomy and independence;
- internal audit effectiveness;
- compliance and director access to data and information;
- root cause analysis including appropriate remediation; and
- investigations of misconduct.

The DOJ's additional guidance on how it evaluates corporate compliance programmes demonstrates there are numerous opportunities for forensic accountants working with legal and compliance teams to add significant value in building and enhancing the corporate compliance function.

Preservation, mitigation and stabilisation 22.3

Turning to the specific steps where a forensic accountant can assist, an important consideration at the outset of an investigation is to identify the necessary steps to mitigate loss of funds or other assets and to preserve data and relevant records. This may entail closing of bank accounts, freezing of email and other communications, deactivating user passwords and other steps to deny access to subjects of the investigation. Where the nature of the investigation requires it, financial and accounting information will need to be preserved and stabilised. Physical documents in this category may include a wide variety of records, such as purchase orders, invoices, customer orders, delivery records, etc. Every step of the transaction cycles involved in the scheme under investigation should be considered at this stage to identify all potentially relevant documents and electronic records (including audio).

See Chapters 5 and 6 on beginning an internal investigation

e-Discovery and litigation holds 22.4

Owing to the proliferation of electronic data, an increasingly important early step in many investigations is to determine what relevant information exists, in what form (paper or electronic), where it is located (e.g., an on-site data centre, off-site at vendors, in the cloud), what security measures are in place over the data, and what the organisation's standard record retention and destruction policies and practices are. The process of identifying, taking inventory of, and preserving relevant data that may be of use in an investigation is often referred to as e-discovery.

In addition, as soon as it becomes apparent that an investigation is necessary, a litigation or preservation hold notice should be issued. These notices require the suspension of any destruction or deletion of paper or electronic records that could be relevant to the investigation. Proper communication of a litigation hold or preservation order to all pertinent individuals and department which may include third parties who, for example, are responsible for archiving the organisation's data off-site, is important to avoid accidental destruction of critical records.

© Law Business Research 2021

22.5 Violation of internal controls

An important part of an investigation is establishing whether the act was intentional. Demonstrating that a subject was aware of and violated a documented, well-established internal control is often a relevant factor. For example, determining how an internal control was circumvented or otherwise violated is also an important part of understanding how fraud or corruption was perpetrated, because establishing that a subject intentionally violated internal controls can be important in connection with criminal prosecution or the regulatory enforcement process, and understanding precisely how internal controls were violated is critical to developing a remediation plan to enhance controls and to prevent future occurrences. In addition, understanding how internal controls were bypassed or overridden will often provide critical insight into who knew what and when.

The first step in determining whether policies or procedures were violated is to gain a thorough understanding of the accounting behind the controls as well as the identities of employees responsible for accounting, internal controls and the business processes being investigated. Upon gaining this basic knowledge, we identify the established policies and procedures (the current state). This normally entails reviewing documented policies and procedures, and walk-throughs, and may also include interviews with employees to help clarify any ambiguities in the documentation. Some considerations include:

See Chapters 7 and 8 on witness interviews

- which employees are authorised to initiate and process a transaction;
- which employees are authorised to approve a transaction;
- which employees can approve new vendors;
- which employees are responsible for account reconciliations;
- which employees have physical access to assets, including cash;
- documentation requirements for the transaction;
- how and where electronic and paper records are stored; and
- how exceptions or unusual transactions are handled, including budget variance analysis.

It may also be important to review any training programmes that the subject of the investigation has received. Doing so can establish more firmly that the subject had an understanding of the proper method of handling the transactions.

Most accounting cycles, such as procurement, disbursement of funds and payroll, include many steps. Some of these are evidenced manually, such as with written approvals by signature and supporting documents such as invoices and delivery confirmations. Other steps require analysis of electronic records. Examples of critical pieces of electronic evidence related to internal controls include:

- *Date and time stamps*: Most systems leave a valuable trail that can be used to establish an accurate and detailed timeline of events. For example, a vendor invoice may be put into the accounts payable system late at night during non-work hours, approved for payment moments later and payment is made to the vendor the very next day. Why the rush? Is there a legitimate need

© Law Business Research 2021

or is something more devious involved? Does payment so quickly comply with the organisation's normal cash management and bill-paying policies?

- *User identification numbers*: Systems maintain a record of user log-ins, along with date and time of information access and updates. Directly or indirectly, it is often possible to determine exactly which user of a system performed each step in the chain of activities comprising a transaction – who set a vendor up in the master file, who authorised the purchase and whether it was competitively bid, who entered the vendor invoice, who approved it for payment, who scheduled it for disbursement, who transmitted payment, etc.
- *Security matrices*: Often reviewed in connection with the preceding step, determining which users have access to specific components of each system can play a vital role in assigning responsibility for specific steps in a matter under investigation. Access to a system often does not mean access to every part of that system. Analysis of a security matrix provides details of this information. Who has 'read only' access to vendor and invoice data? Who has input capability? Who has approval authority to release payments to vendors? Aligning this information with information gleaned from the preceding steps can find exactly where internal controls were compromised, including identification of instances of unauthorised access through password theft or sharing.

Physical documents are often important pieces of evidence in an investigation. But electronic evidence associated with a transaction cycle tends to be equally or more important. Proper analysis of this evidence enables an investigator to draw conclusions and gain insight that would be impossible in an entirely paper-based system. For example, a paper copy of a vendor invoice can be analysed to establish whether a subject signed or initialled it, and perhaps whether any alterations were made to the document. But if the organisation's vendor invoice approval and payment system is electronic, the investigator can also determine with precision the date and time of the approval of the invoice and perhaps even where the subject performed these steps (from home, from a workstation in the office, etc.).

Forensic data science and analytics 22.6

Forensic data science refers to using a scientific method for the identification, collection, analysis and reporting of electronically stored information (ESI). This includes both structured data, such as financial records in a database, and unstructured data, such as files on a file server. The most commonly analysed data in forensic accounting investigations are financial, but several non-financial categories of data are also very useful to investigators. Each is explored below.

Data analysis generally has three applications in the investigative process:

- to initially detect fraud or non-compliance (e.g., monitoring performed by internal audit);
- to corroborate an allegation in order to justify launching an investigation (e.g., proving that an allegation received via a hotline appears to have merit); and

© Law Business Research 2021

- to perform certain parts of the investigation (e.g., analysis of payments made to suspicious vendors).

Each of these will be explained further. But first, a few important points about data analytics are essential.

Data analytics rarely prove that fraud or non-compliance occurred. Rather, data analysis identifies transactions or activities that have the characteristics of fraud or non-compliance, so that they can be examined further. These are often referred to as anomalies in the data.

If an investigation ultimately leads to employee terminations or legal proceedings to recover losses, it is critical to have properly analysed the anomalies that data mining has identified. Could the anomaly in the data, or an anomaly in a document, while often identified as a characteristic of fraud, also simply indicate a benign deviation? Failing to investigate and rule out non-fraudulent explanations for anomalies can have consequences that many investigators have learned about the hard way.

Identifying and exploring all realistically possible non-fraudulent, non-corrupt explanations for an anomaly is also called reverse proof. Examining and eventually ruling out all of the valid possible non-fraudulent explanations for an anomaly in the data or documentation can prove that the only remaining reasonable explanation is fraud or corruption.

Careful consideration of alternative theories for data and document anomalies is critical to protecting the organisation and the investigator from liability stemming from falsely accusing someone of wrongdoing.

22.6.1 Data mining to detect fraud or non-compliance

Depending on which application or phase of the investigative process is involved, the nature of forensic data analysis can vary. For example, as an initial detector of fraud or non-compliance through ongoing monitoring, forensic data analytics usually takes one of two broad, but opposite, approaches: identification of any activity that deviates from expectations, or identification of activity that possesses specific characteristics associated with fraudulent or corrupt behaviour or other non-compliant conduct.

The former approach is taken when acceptable behaviour is narrowly defined, such that the slightest deviation warrants investigation. The latter approach is the more common. It is driven by a risk assessment and is based on what this type of fraud or non-compliance would look like in the data. For example, a shell company scheme might evidence itself by an address in the vendor master file matching an address in the employee master file. Any instances of such a match would be investigated.

In some cases, basing the 'investigate' or 'don't investigate' decision on a single characteristic in the data can result in numerous false positives. For this reason, more sophisticated data analytics often rely on the consideration of multiple characteristics in assessing the risk of activity being fraudulent or corrupt. These characteristics can be combined into a singular risk score per

© Law Business Research 2021

transaction that can be aggregated by vendor, geography or other grouping. Risk scoring or risk ranking transactions can be useful for prioritising where to focus in the data.

Regardless of which of these two approaches is taken, data analytics often represents an essential tool for gathering evidence to lay the foundation for substantive examination of books, records and other evidence. Following the reverse-proof concept described above is critical once anomalies indicative of possible wrongdoing are uncovered.

Corroborating allegations 22.6.2

As a method of corroborating an allegation that has been received, data analysis can be of great value. It is a significant advantage to the investigator because, more often than not, it can be performed on electronic data without alerting the subject of the allegation. In this application, the allegation is first assessed in terms of what impact the alleged fraudulent or corrupt act would have on financial or non-financial data. It is important to understand how data flows through the organisation from the point of origination, through multiple hops in different departments, for example how an invoice will flow from a business unit to finance and back to the business unit. The data can change quite a bit throughout different business processes and this will need to be understood for a robust analysis of it. To illustrate, take the example of an allegation that workers in the shipping department of a warehouse are stealing inventory by short shipping orders to customers. There are numerous sources of data, both financial and non-financial, that could be analysed to assess the validity of this allegation:

See Chapters 19 and 20 on whistleblowers

- gross profit margins – an unexplained decline in gross profit margins by product, or by location (as a result of having to re-ship additional items, with no associated revenue, to satisfy the customer);
- inventory purchases – unexplained increases in purchases of certain inventory items without a corresponding increase in sales;
- customer complaints – customer service data indicating complaints about incomplete shipments, especially if those complaints can be correlated back to specific orders; and
- shipping records – using the customer complaint data, orders are correlated to specific shipments and employee names associated with filling and shipping these orders. Shipping records might also reveal more shipments to a customer than orders, indicating a second shipment was needed to complete the order after the customer complained.

This is a simple example, but one that illustrates that for every allegation, there likely exists data associated with either the perpetration or concealment of the fraud or non-compliance. And this data normally exhibits one or more anomalies in comparison with data from similar transactions that do not involve fraud or non-compliance.

© Law Business Research 2021

22.6.3 Using data analysis in an investigation

The final application of forensic data analysis is performed during the investigation itself. Once an anomaly has been found to involve fraud or non-compliance, additional forensic data analysis, along with substantive forensic examination of the evidence, may be performed to:

1 determine how long the activity has occurred;
2 determine which employees (or third parties) have participated in the fraud (i.e., assessing whether collusion was involved);
3 measure the financial damage resulting from the activity;
4 identify other fraudulent or corrupt conduct by the same individuals; and
5 determine how the fraudulent or corrupt act was concealed and how internal controls were circumvented.

Determining who is involved in the fraud as well as who possessed knowledge of it is critical to the mitigation and control enhancement objectives. According to a 2020 report by the Association of Certified Fraud Examiners (ACFE), nearly 51 per cent of all fraud and corruption schemes investigated involved multiple perpetrators.[4] Typically, losses tend to increase with multiple perpetrators, particularly when three or more individuals conspire to commit fraud. This figure has been steadily rising since the ACFE began studying fraud. The 51 per cent statistic is divided nearly evenly between cases involving multiple internal perpetrators and those involving collusion between insiders and outsiders, such as vendors or customers.

Point 4, above, may also come as a surprise to some. The ACFE report indicates that 35 per cent of occurrences of fraud (especially with respect to asset misappropriations) are perpetrated through multiple methods. The allegation or investigation may have initially focused on only one specific method. Exploring what other activities the subject might have the capability of engaging in is an integral element of the investigation. Investigators and victims attempt to 'put a fence around the fraud' as early in the investigative process as possible. Understanding the responsibilities of the subject and the potential for unrelated schemes is essential for erecting the fence. Victims often desire a narrow investigative scope – a sort of wishful thinking. An investigator's worst-case scenario is missing a scheme conducted by a subject despite investigating the subject.

The question of who knew what and when can be particularly important in satisfying auditors in the context of financial reporting fraud. In addition to quantifying the financial statement impact from fraud, auditors rely on representations from management. Knowledge of whether previous representations

4 2020 ACFE Report to the Nations on Occupational Fraud and Abuse, published by the Association of Certified Fraud Examiners, available at https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf.

© Law Business Research 2021

came from fraudsters and the auditor's assessment of management's integrity are often important aspects of financial reporting fraud investigations.

In the next sections, the distinction between financial and non-financial data will be explored, followed by a discussion of internal versus external data.

Analysis of financial data 22.7

Most analyses of internal data relevant to an investigation begin with financial data, much of which comes from the organisation's accounting system. Accounting data can exist in several separate systems, such as:

- general ledger, the master ledger that reflects all accounts and the sum of all accounting activity for the organisation;
- general journal, where journal entries are initially recorded before being posted to the general ledger;
- books of original entry, which contain details of certain types of financial transactions, summaries of which are posted to the general ledger. Examples of books of original entry include sales, cash receipts, cash disbursements and payroll; and
- subsidiary ledgers, which contain additional details of transactions and activities that appear only in summary form in the general ledger. Examples of subsidiary ledgers are accounts receivable and accounts payable ledgers.

Performing an investigation often requires the extraction and analysis of data from all these systems to see the big picture or to properly trace the history of a transaction or series of activities. The days of manually maintained books of original entry are gone. The vast majority of organisations now use electronic accounting and financial software, and in larger organisations these systems are included as part of a broader ERP (enterprise resource planning) system.

Some systems are hybrids of financial and non-financial information. Examples of these systems include the following:

- *Inventory*: In addition to cost information associated with purchases, the system may also provide data on quantities and dates of purchases, deliveries, shipments, inventory damaged or scrapped, and counts resulting from physical observation.
- *Payroll*: In addition to data on net amounts paid to employees, the payroll system will usually include other relevant data needed to calculate an employee's gross and net pay, including various worker classification codes, hours worked during a pay period, rates of pay, tax and withholding information, along with bank account information for the electronic transfer of funds to employees.
- *Human resources*: In most large organisations a human resources system that is separate from payroll is maintained. Included in this system are data on rates of pay and past raises, incentive payments, and other financial data about each employee, as well as significant amounts of non-financial data, such as each employee's home address. Human resource information systems may also include vital information associated with an employee's

© Law Business Research 2021

initial hiring, such as background and reference checks, verification of information provided on an employment application, etc. This information can be important if the organisation anticipates filing an insurance claim to be indemnified for losses attributable to an employee.

Availability of and legal considerations associated with each of these sources of internal data vary from one jurisdiction to another, particularly with respect to payroll and personnel information. Privacy issues must be considered before embarking on any use of such data in an investigation.

22.8 Analysis of non-financial records

Increasingly, non-financial data is being analysed as a standard element of an investigation. Non-financial data can be classified into two broad categories: structured and unstructured.

Structured data is the type of data that generally conforms to a database format. It is often numeric (e.g., units in inventory, hours worked by an employee, calendar dates), but can involve alpha data as well (e.g., codes associated with types of customer or employee, certain elements of an address).

Structured non-financial data is found in many systems, including those that include financial data mentioned above. Other systems, however, are entirely non-financial, but provide data that can be important to an investigation. Examples of non-financial systems commonly used for investigative purposes include the following:

- *Security*: Many organisations now use tools that leave an electronic trail of the exact times and dates when specific employees entered or left the building. Records of visits by vendors and other visitors may be included in this system or may be kept separately. Security information can be very useful in establishing timelines or the whereabouts of specific individuals.
- *Network data*: Much like accessing a building, networks maintain electronic records each time an authorised user logs on or off the system, and may retain a record of various aspects of the user's network activity, such as which folders were accessed, which data was downloaded, which systems were used, etc.
- *Customer service*: As the earlier example illustrates, data collected in the customer service system can have numerous applications in an investigative setting. Customer complaints about items missing from their orders may indicate theft in the warehouse.

Unstructured data refers to data that does not readily conform to a database or spreadsheet format. Text associated with messages in emails, explanations for journal entries and other communications are the most common. Unstructured data also includes photographic images, video and audio files.

Emails and text messages of interest to an investigator may involve messages within the organisation, between employees and communications between organisation employees and vendors, customers or other third parties.

© Law Business Research 2021

Similar to other electronic data, when a user 'deletes' this information, a backup or archive version is often left behind and is available to an investigator. Understanding an organisation's backup, archiving and storage practices is crucial to this part of an investigation.

Careful reviewing of email, instant messaging or text message chains (and, if available, recordings of telephone calls) is vital to most investigations and can provide an investigator with vital clues, such as:

- the timeline of events;
- the level of knowledge of events that specific individuals may have had;
- the extent of collusion among individuals;
- whether a subject or witness deleted email evidence; and
- whether there are indications of intent.

Establishing a timeline can be one of the most important requirements of an investigation. A complete timeline of events can often be established by integrating the separate timelines learned from a review of:

- systems and facilities access records;
- electronic transaction information (e.g., entries, approvals);
- documentation (e.g., invoices, shipping records); and
- electronic communications, including metadata (e.g., emails).

Email review is of particular importance in establishing intent. Intent, particularly to a civil standard, may be inferred from communications that indicate an awareness that planned transactions or activities are in conflict with established policies and procedures or treatment of similar transactions. Email, although a rich source of behavioural history, can quickly become overwhelming from a volume standpoint. There are many modern techniques for prioritising and culling this type of information. Sentiment analysis, a form of artificial intelligence (AI), can assist with identifying the writer's emotional state. Other forms of AI, typically referred to as natural language processing (NLP), can help correct for potential biases that investigators naturally bring to their review. For example, an investigator may select a list of search terms to run against email data to reduce the population for further review and bring the most important messages to the forefront. By creating these search terms, the investigator has leveraged what he or she knows about the case and this inflects a natural bias. By using AI and NLP, the data is allowed to speak for itself, and computer algorithms will cluster statistically relevant information. Typically, a combination of search terms and NLP is used. These types of analyses can identify pressures or rationalisations associated with fraudulent or corrupt behaviour. For example, an employee stating in communications that he or she feels unfairly treated or resentment towards management might be expressing a rationalisation for stealing from an organisation.

One example of the use of both financial and non-financial data is in the investigation of alleged financial reporting fraud. When an allegation is made that a company's financial statements have been intentionally manipulated, any

© Law Business Research 2021

of a large number of schemes come to mind. The most common fraudulent financial reporting schemes involve improper recognition of revenue, inflating turnover or sales through fictitious transactions or accelerating the recognition of legitimate transactions. So, a revenue inflation scheme will serve as our example.

To establish that the financial statements improperly reflect sales, electronic data from the sales and accounts receivable systems will need to be analysed in conjunction with physical or electronic records associated with customer orders, inventory, shipping and delivery, among others. By analysing these records, the investigator may establish that sales recognised by the company failed to conform to applicable accounting standards (e.g., International Financial Reporting Standards).

But accounting mistakes are common. For this scheme to be fraudulent, the subjects' dishonest intent to violate the accounting rules must be established. This is where analysis of emails and other electronic communications may be valuable. Perhaps email exchanges can be located documenting discussions of revenue shortfalls and methods of meeting budgeted figures. In this case, analysis of unstructured non-financial data may be one of the keys, along with interviews of subjects, to proving that the company intentionally violated their own policies and pertinent accounting principles.

Analysis of both financial and non-financial data is an important step in preparing to interview witnesses and subjects. Reading email and other communication chains before conducting the interview allows an investigator to plan the order and structure of questions to put the interviewer in the best position to identify conflicting statements and to obtain a confession.

Other investigation scenarios in which analysis of unstructured data association with communications between individuals include:

- collusion between multiple employees involved in the theft of cash or other tangible or intangible assets;
- bribery schemes in which the organisation has paid bribes, directly or indirectly, to obtain or retain business; and
- kickback schemes in which a vendor has paid a procurement official of the organisation to steer business to the vendor.

22.9 Use of external data in an investigation

Most data and documentation used in an investigation is internally generated – it comes from within the organisation or (in the case of invoices from a vendor) is otherwise readily available within the organisation. Occasionally, however, data or documentation that is only available from external sources becomes essential. External sources of data fall into two broad categories: public and non-public.

Public data and documents are those that are usually available to the general public either by visiting a website or facility or on request from the holder of the records. In most cases, public records are maintained by government

© Law Business Research 2021

agencies. Examples of public records vary significantly from one jurisdiction to another, but some that may be useful to investigators are:

- licences and permits issued by government agencies to individuals or businesses;
- records of ownership or transfers of ownership of property (e.g., sales of land and buildings);
- criminal convictions of individuals and organisations, and certain other court records; and
- business registrations and certain filings made by organisations.

Availability and the extent of these records can differ markedly as an investigator seeks information from different parts of the world.

Increasingly, public records may also include information that an individual voluntarily makes publicly available. For example, when an individual posts photos or makes statements on social media, this information might be readily available to any and all viewers. Once again, investigators should always use caution when accessing this information, especially if the information is only available to 'friends' or other contacts that the individual has granted special access to. But when social media information is made fully available to the general public, it can provide a treasure trove of information about a subject, such as:

- places the subject has visited;
- individual contacts;
- business relationships;
- assets owned; and
- past and present employers.

Another public source of information involves websites that do not require special password or other access privileges. For example, a company's website, or that of a trade association or other membership group with which a subject might be involved, could provide clues about the subject's relationships, travels and past.

Even information that is no longer on a website might still be available to an investigator. The Wayback Machine at www.archive.org is an archive of more than 600 billion past pages on the internet (as at November 2021). Simply typing the URL of a website into the Wayback Machine will produce an index by date of prior versions of that website which have been archived and are available for viewing. Accordingly, an investigator may be able to find useful information from past editions of websites long after the information has been deleted.

Non-public records are private and confidential. Holders of these records are under no obligation to produce these records unless they have provided their consent or they are compelled to do so as a result of a legal process, such as a court order or subpoena. Records such as personal bank statements of individuals who may be the subject of an investigation fall into this category. Investigators normally do not have ready access to these records.

© Law Business Research 2021

Another challenging and practically untraceable medium adopted by cybercriminals is the dark web, a small section of the deep web (content on the internet that is not readily accessible or visible through search engines) designed so it cannot be accessed through standard web browsers. It allows anonymous private communications for legitimate reasons (e.g., protection of free speech), but also for the distribution of harmful information and purchase of illegal goods and services that law enforcement agencies have difficulty tracing. For example, once an organisation's network has been breached, the intruder may extract sensitive information such as customer data, logins and passwords, banking details, taxpayer identification and social security numbers, and credit card details, and then sell this confidential information anonymously on dark web marketplace and forum websites to buyers across the world.

There are no anti-money laundering or know-your-customer (KYC)controls on the dark web. Most dark web sites are anonymous and difficult to attribute to an owner because these sites use a '.onion' domain suffix, which can only be accessed via a Tor (The Onion Router) browser. Website traffic is bounced through randomly selected Tor entry, relay and exit nodes using separate embedded layers of data encryption for each hop in the network circuit (hence the term 'onion'). In addition, perpetrators are increasingly using cryptocurrencies to conduct illicit financial transactions via the dark web while hiding their identities.

Dark web investigations therefore require specialist forensic investigative tools, such as a secure dark web browsing platform with network and malware protection (e.g., firewalls and virus scanning), and secured data storage that maintains a strong custody chain for digital evidence, backed by strict and auditable compliance controls. Such tools can be used to search and monitor dark web communications, capture cryptocurrency information (e.g., block-chain wallet addresses) and attempt to identify and locate cyber fraudsters while capturing and analysing digital evidence in a forensically sound manner.

When assisting counsel with preparing a request for a subpoena or other court-ordered production of private records, an investigator should be as detailed and specific as possible. Overly broad requests are normally either denied or result in potentially lengthy delays. The format of the records and the tools available to the investigator to analyse them should also be considered. For example, if records associated with a bank account are requested, rather than requesting 'all records associated with the account', it is normally better to itemise a list of those records, such as by requesting copies of:

- bank statements for the relevant period;
- images of cleared checks;
- supporting documents for other debits from the account;
- signature cards; and
- application or other forms prepared to open the account.

A vendor's internal records would normally be non-public and the vendor may be under no obligation to provide them to an investigator. However, a properly worded right to audit or access to records provision included in the

© Law Business Research 2021

contract between the organisation and the vendor may provide access to some of the most important records an investigator might need if fraud or corruption involving a vendor is suspected. A well-crafted access-to-records clause can enable an investigator to request and view a wide variety of records, including:

- supporting documentation for invoices sent to the organisation by the vendor;
- accounting and payroll records;
- time records supporting employees' work efforts; and
- communications relevant to the vendor's relationship with the organisation.

If a vendor is suspected of inflating their billings to the organisation in any manner, or there are indications of collusion between an organisation employee and a vendor, one of the first steps an investigator should perform is to carefully review the terms of the contract to assess the organisation's rights to access these records.

Review of supporting documents and records 22.10

Studying the processes and internal controls involved in the transaction cycle in the investigation and the results from data analytics and email review will result in a population of documents and electronic records that are relevant. For example, in a corruption investigation, several paper documents or records may need to be reviewed:

- budgets;
- agent, distributor, supplier and customer contracts;
- bidding documents;
- margin data;
- price lists;
- market data;
- vendor set-up documents;
- sales by region, agent, territory and product;
- background checks;
- purchase order or purchase request;
- bill of lading or other confirmation of delivery of goods;
- signed confirmation for services provided;
- invoice from a vendor or supplier;
- cheque or disbursement request form; and
- banking records.

These records might be reviewed for many different reasons. Among the most common are:

- establishing a timeline of events;
- testing their clerical accuracy;
- reviewing for inconsistencies, anomalies and trends;
- reviewing for agreement with accounting records;
- reviewing for compliance with internal controls; and

© Law Business Research 2021

- determining authenticity of the document, the vendor and the services rendered.

Testing for authenticity of the record itself or of individual signatures on documents normally involves a highly specialised skill, unless an anomaly is obvious. Accordingly, if an investigator suspects that a document on file is fraudulent or has been physically altered, or that a signature is not authentic, the document should be protected until someone with the specialised skills necessary can assess its authenticity. Examples of obvious deficiencies in documentation include:

- inconsistencies in addresses;
- lack of letterhead or other characteristics normally expected of a legitimate vendor;
- misspellings or other typographical errors;
- document at variance with vendor master file;
- inconsistencies in dates; and
- inconsistencies in vendor invoice numbers and sequencing.

In a corruption investigation, the authenticity or business purpose of an intermediary may be in question. The investigator should determine:

- the purpose of the intermediary;
- the principals behind the intermediary;
- the value, if any, of services rendered by the intermediary, to rule out use of the intermediary to create a slush fund or otherwise bribe a customer or influencer;
- life before or after the intermediary; and
- if the company documentation in connection with the intermediary is consistent with other intermediaries, policies and best practices.

22.11 Tracing assets and other methods of recovery

If the subject has misappropriated cash (via intercepting incoming funds intended for the organisation, stealing cash on hand, or fraudulently transferring funds from the organisation in connection with a disbursement fraud) one of the goals of most investigations is to secure the return of the funds. To do so, the investigation team must determine what the subject did with the money. Other sources of recovery may include culpable outside parties, including but not limited to collusive vendors, customers and agents. Coverage for employee dishonesty losses under insurance policies and fidelity bonds may also be possible.

If the subject misappropriates other assets, a similar question must be addressed – where are they? Often, when assets are stolen, the subject's goal is a conversion to cash by selling the stolen assets. In other cases, the stolen asset itself may be of use to the subject.

Depending on how assets were stolen, varying degrees of a trail might be left by the perpetrator, enabling the investigation team to forensically determine the flow of money after it has left the organisation. The trail may begin with the company's books and records. However, it is usually intentionally made opaque

© Law Business Research 2021

by fraudsters through money laundering techniques such as layering, transfers to shell companies, nominee shareholders and the use of clandestine communication techniques, cryptocurrencies, and tax havens where criminal law enforcement assistance may be less effective. Many of the records necessary to fully trace assets are non-public. But investigators are sometimes surprised to learn that a subject has left a public trail of valuable clues regarding the disposition or location of illegally obtained funds or assets that can be identified through indirect techniques, such as social media and internet due diligence, interviews of people in the know, establishing connections to the fraudster's other assets in more vulnerable venues and through multinational co-operation of law enforcement agencies.

Cryptocurrencies 22.12

Cryptocurrencies present unique challenges and new opportunities for investigators seeking to trace them and attempt their recovery. Bitcoin, Ethereum and many other emerging cryptocurrencies are easily accessible and widely accepted to the degree that fraudsters can, with minimal effort and risk, rely on them to move funds for the same purpose fiat currencies have long been used to transfer and conceal the source, nature and ownership of illicit funds. The added advantages of cryptocurrencies not requiring physical contact or interaction with banks has made them the payment method of choice for perpetrators of ransomware attacks and other schemes aimed directly at defrauding victims (e.g., internet-based advanced fee schemes). Therefore, forensic investigators must still follow the money trail and will be doing so more often with cryptocurrencies; however, there is another side to the coin, so to speak. While cryptocurrencies provide a degree of pseudonymity, especially those designed to provide enhanced privacy (e.g., Monero, Zcash), they do not provide complete anonymity. On the contrary, cryptocurrencies by design create an immutable public blockchain record of transactions that investigators can exploit to follow the money to a certain extent, provided they have the right tools and training.

As new cryptocurrencies are developed on different blockchains, investigators must also learn to follow transfers across them because fraudsters are already using cross-chain transfers to launder funds. This also requires the investigative blockchain data analysis tools (e.g., TRM Labs, Chainalysis) to be continually adapted and advanced to enable cross-chain analysis.

Although the on-blockchain transactions in cryptocurrencies can be traced using public blockchain data, for digital asset tracing to be successful for asset recovery or prosecution purposes investigators must be able to trace transactions beyond the blockchain to identify the counterparties and the ultimate beneficiaries. This requires identifying and pursuing additional information from virtual asset service providers (VASPs) such as cryptocurrency exchanges, hosted wallet platforms and financial institutions providing custodial services for cryptocurrencies – the on-ramps and off-ramps to blockchains. These entry and exit points for cryptocurrencies are essential to fraudsters because for cryptocurrencies to be more useful to the ultimate beneficiaries, the digital asset value must

© Law Business Research 2021

still be converted to or from fiat currency, or other tangible assets. Therefore, a key goal of blockchain data analysis is to correlate known blockchain addresses for on-ramps and off-ramps with blockchain data on suspect transactions to develop leads as to where cryptocurrency funds were converted. If this was a legitimate or regulated VASP, KYC information may have been recorded and more traditional investigative steps could be followed, such as the use of subpoenas, search warrants, regulatory inquiry or examination, witness interviews, etc.

A challenge for cryptocurrency-related investigations is the existence of illicit, unlicensed peer-to-peer exchanges that offer a way to convert fiat currencies to and from cryptocurrencies through unregulated entities that do not collect KYC information. There are also providers of cryptocurrency laundering services known as 'mixers' that offer a way for money launderers to obfuscate the actual parties to a blockchain transaction by mixing the cryptocurrency value with large numbers of other blockchain transactions going through the mixer. Even transactions flowing in and out of a legitimate exchange can become untraceable using blockchain data (without co-operation from the exchange to obtain internal account data) due to the sheer volume of transactions flowing through a large exchange (e.g., Coinbase).

In summary, investigating financial crimes involving cryptocurrency and digital asset tracing will require specialist blockchain analysis and intelligence tools and services, as described above, to identify leads to follow beyond the public blockchain. This may be easier to do when dealing with cryptocurrency compared to fiat currency that is physically transferred, but it also presents new challenges. Understanding these challenges and how to identify potential sources of additional attribution data for cryptocurrency transactions is essential. This will continue to be a changing landscape for investigators given the continually evolving technology and expanding array of new forms of blockchain based cryptocurrencies and emerging decentralised finance (DeFi) platforms that promise to offer an even greater variety of financial services based on blockchain technology.

22.13 Conclusion

The rapid conversion of accounting and other records from paper-based systems to electronic systems, coupled with the explosion in the quantity and types of electronic data, has resulted in many changes in the field of forensic accounting and the requirements for investigations. Expertise in the evaluation and handling of electronic evidence is just one way in which forensic accounting has evolved. Focused and efficient use of data analytics as well as the ability to mine a universe of publicly available yet critical information regarding subjects, companies and their relationships are two additional ways in which forensic accounting has matured. On the other hand, operating within a web of global data privacy and other complex regulatory constraints can complicate the job of the forensic accountant. All in all, today's forensic accountants are significantly more successful in identifying, investigating and mitigating fraud than their counterparts in the past.

© Law Business Research 2021

23

Negotiating Global Settlements: The UK Perspective

Nicholas Purnell QC, Brian Spiro and Jessica Chappatte[1]

Introduction 23.1

This chapter discusses the three main options that corporates typically consider when they are seeking to settle criminal and related proceedings in England and Wales – negotiated plea agreements, civil recovery orders (CROs) and, as of 24 February 2014, deferred prosecution agreements (DPAs).

Central to any consideration of criminal settlements in England and Wales is the identification principle under the common law, which defines the scope of corporate criminal liability. The principle states that the 'acts and state of mind' of only those who represent the 'directing mind and will' of the corporate will be imputed to it.[2] The application of this principle is generally restricted to the actions of the board of directors, the managing director and other senior officers carrying out managerial functions and acting and speaking as the corporate.[3] The identification principle has historically made it, and continues to make it, very difficult for authorities in the United Kingdom to convict corporates of any significant size.[4] The English courts have, in certain situations, applied this

1 Nicholas Purnell QC is head of Cloth Fair Chambers. Brian Spiro is a partner and Jessica Chappatte a senior associate at Herbert Smith Freehills LLP. The authors wish to acknowledge the contribution of Rod Fletcher to this chapter in previous editions, a partner at Herbert Smith Freehills LLP until his untimely death in November 2019.

2 *Lennards Carrying Co v. Asiatic Petroleum* [1915] AC 705, *Bolton Engineering Co v. Graham* [1957] 1 QB 159 (per Denning LJ) and *R v. Andrews Weatherfoil* [1972] 56 Cr App R 31 CA.

3 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153.

4 See *R v. Barclays Plc and Barclays Bank Plc* [2018] (Southwark Crown Court) and *The Serious Fraud Office v. Barclays Plc & ANR* [2018] EWHC 3055 (QB), in which the alleged guilt of senior executives of Barclays Plc, including the former chief executive officer and the chief financial officer, could not be attributed to the bank in circumstances where the board

© Law Business Research 2021

rule of attribution to persons outside the board level, but this will depend on the construction of the particular offence in question.[5] This relatively narrow position should be contrasted with that in the United States, where corporates may be vicariously liable for the acts of their employees. This difference in the probability of a successful prosecution explains, in part, why settlement agreements are far more prevalent in the United States than in the United Kingdom.

The statutory landscape in the United Kingdom is changing to make the prosecution of corporates easier for authorities. Section 7 of the Bribery Act 2010 created criminal liability for corporates who fail to prevent 'associated persons' (potentially including agents, subsidiaries and other third parties as well as employees) from committing bribery. The Criminal Finances Act 2017 includes a similar offence of failure to prevent the facilitation of tax evasion. Under this offence (which came into force on 30 September 2017) prosecutors will need to prove that tax evasion has occurred, that a person facilitated this evasion and that the facilitator was a person associated with the accused corporate. This type of offence of 'failure to prevent' may become increasingly common. The former Director of the Serious Fraud Office (SFO), Sir David Green QC, called on a number of occasions for the failure-to-prevent offence to apply to all financial and economic crimes and in early 2017 the Ministry of Justice called for evidence in relation to the introduction of such an offence (the Call for Evidence). The current Director of the SFO, Lisa Osofsky, has also expressed her frustrations at the United Kingdom's 'antiquated' system for prosecuting corporate fraud, which she has said is 'so complicated' that it can 'make identifying responsible individuals challenging or impossible' and thereby creates a 'dangerous culture of organised irresponsibility' instead of encouraging 'offending companies to uphold the law and become good corporate citizens'.[6] In March 2019, the UK Parliament's Treasury Select Committee published a report following its economic crime inquiry,[7] which included suggestions received from the SFO either to replace the identification principle with a form of vicarious liability[8] or to introduce a new offence of failing to

retained control of the transactions and the bank exercised robust corporate governance. Although these judgments date from 2018, reporting restrictions applied while criminal proceedings continued against three former executives of the bank who were charged with conspiracy to commit fraud arising from their actions in the Barclays capital raisings of 2008. The restrictions were lifted in February 2020 following their acquittal.

5 *Meridian Global Funds Management Asia Ltd v. Securities Commission* [1995] 2 AC 500 PC.

6 Lisa Osofsky, 'We're defending the UK as a safe place for business', *The Times* (30 Jun. 2021), https://www.sfo.gov.uk/2021/06/30/were-defending-the-uk-as-a-safe-place-for-business

7 https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/report-published-economic-crime-17-19/.

8 The SFO's proposal was that a company would be guilty of an offence if a person associated with it commits the relevant offence intending to obtain or retain business for the company; to obtain or retain a business advantage for the company; or otherwise to benefit the company (financially).

© Law Business Research 2021

prevent economic crime. The committee made no recommendation as to which suggestion it preferred but appears to have favoured extending the failure-to-prevent offence.[9] The Ministry of Justice published its long awaited response to the Call for Evidence on 3 November 2020 in which it did not reach any definitive conclusion on the way forward for reform.[10] It found that the responses to the Call for Evidence did not provide a conclusive evidence-base on which to justify reform, but raised important questions, in particular about the operation of the identification doctrine. Accordingly, the Ministry of Justice requested a review of the identification doctrine by the Law Commission, which opened a consultation on the law relating to corporate criminal liability, seeking responses from 9 June to 31 August 2021 and, following an analysis of these, will publish a paper on the options for reform of the law. If a broad failure-to-prevent offence for all financial and economic crimes is introduced (whenever that may be), this will inevitably lead to an increase in the prevalence of settlements of criminal proceedings in England and Wales.

Each option for settlement currently available to a corporate has its own particular advantages and disadvantages, but a common feature is that they are all jurisdictionally limited in their effect to the United Kingdom. Where there are multiple investigating authorities from different jurisdictions, settlement negotiations in the United Kingdom will typically be approached as part of a larger, overarching strategy to settle current and prospective proceedings globally.

UK authorities are increasingly participating in global settlements, particularly with their US counterparts. It may yet be too early to identify any trends, although one distinct feature has emerged: the central role of the UK judiciary. The *Innospec* settlement was criticised by the senior judge who heard the case, Lord Justice Thomas, for being presented as a 'done deal',[11] and the DPA model introduced in the United Kingdom departs significantly from its US counterpart by being conditional on substantial judicial review and approval.[12]

9 See comments made by a specialist legal adviser to the committee, available at https://www.lawgazette.co.uk/peers-call-for-speedier-bribery-investigations-/5069588.article.

10 Ministry of Justice, 'Corporate Liability for Economic Crime, Call for Evidence: Government Response', published on 3 November 2020.

11 *R v. Innospec Ltd* [2010] 3 WLUK 784, [2010] Lloyd's Rep FC 462, [2010] Crim LR 665, paras. 26 to 29 (*Innospec*).

12 Crime and Courts Act 2013 (UK), s.45 and Schedule 17, para. 7.

© Law Business Research 2021

Until the cases of *SFO v. XYZ Ltd (Sarclad)*,[13] *SFO v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc*,[14] and *SFO v. Airbus*,[15] a further feature of settlements concluded by the UK authorities appeared to be that they were more likely to be agreed where the criminal conduct had been contained to an isolated incident. For example, the Balfour Beatty plc settlement (which resulted in the first CRO against a corporate in the United Kingdom) related to one particular contract.[16] The first DPA in the United Kingdom, involving Standard Bank plc (now ICBC Standard Bank plc (Standard Bank)), concerned a particular debt transaction.[17] Similarly, the sixth DPA involving Güralp Systems Ltd (GSL) concerned the company's relationship with one intermediary, Dr Chi, who inappropriately used his position within a government run research institute in the Republic of Korea to assist GSL.[18]

XYZ Ltd (Sarclad) involved an SME that generated the majority of its revenue via sales to Asian markets, through the systematic offer and payment of bribes to secure contracts in a number of foreign jurisdictions over eight years.[19] This conduct could not be said to be contained, involving as it did at least 28 separate contracts, although the misconduct was alleged to have been carried out by a small number of employees. *Rolls-Royce* involved corruption across multiple business lines in seven jurisdictions over the course of 24 years with the involvement of senior management, described in the judgment as 'egregious criminality' involving 'truly vast corrupt payments'.[20] The nature and scale of the conduct in *Airbus* was similar to that in *Rolls-Royce*; the corruption, which was described as being 'endemic' in two core business areas of Airbus, spanned four years and extended to every continent in which Airbus operates.[21] It also involved 'very senior, senior and other employees, including employees with compliance responsibilities'.[22] The tenth DPA, involving Amec

13 *Serious Fraud Office v. XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509 (*XYZ Ltd (Sarclad)*); the company in this case was originally anonymised as 'XYZ' to avoid prejudicing criminal proceedings against individuals arising out of the same facts. Following the acquittals of the individuals, the company was identified.

14 *SFO v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 (*Rolls-Royce*).

15 *Director of the Serious Fraud Office v. Airbus SE* (Case No. U20200108) [2020] 1 WLUK 435 (*Airbus*).

16 'Balfour Beatty plc', press release dated 6 October 2008, SFO.

17 *SFO v. Standard Bank plc (now ICBC Standard Bank Plc)* (Case No. U20150854) [2015] 11 WLUK 804, [2016] Lloyd's Rep FC 102.

18 *Serious Fraud Office v. Güralp Systems Ltd* (Case No. U20190840) [2019] (*Güralp Systems Ltd*).

19 *XYZ (Sarclad) Ltd* (Case No. U20150856) [2016] 7 WLUK 211, [2016] Lloyd's Rep FC 517, paras. 6, 7.

20 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 61.

21 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, para. 64.

22 ibid., para. 65.

© Law Business Research 2021

Foster Wheeler Energy Limited[23] (AFWEL), a UK-based global engineering company[24] that used agents to pay bribes to foreign officials to secure oil and gas contracts in Nigeria, Saudi Arabia, Malaysia and Brazil, also involved a 'scale and duration of corrupt practices', which the court held 'amounted to very significant and systemic corruption'. Whether *Rolls-Royce, Airbus* and *AFWEL* are the high watermark of criminality in corporate settlements remains to be seen, but the trend in these cases suggests that isolated or contained criminality may no longer be an indicator for securing a settlement with UK authorities.

Corporates facing proceedings in more than one jurisdiction could seek to settle each set of proceedings individually, but the concept of a global settlement is to coordinate these negotiations. In theory, a global settlement should be a 'win-win' scenario for both the corporate and the investigating authorities. By acting in concert, the investigating authorities are able to exert more pressure on the corporate to settle than they are likely to do in isolation. For the corporate, a global settlement is potentially a fairer outcome as the penalty will be assessed holistically and also achieves more finality than a domestic prosecution, which confers only limited double jeopardy protection (in those jurisdictions where such protection is granted). As in *Standard Bank*, *Airbus* and *G4S C&J*,[25] in *Rolls-Royce*, the corporate was required under the terms of the DPA to assist law enforcement agencies, regulators and multilateral development banks, including those overseas, at the reasonable request of the SFO. It was also recognised in the judgment that there remained a risk that Rolls-Royce would face liability in jurisdictions not covered by the global settlement involving the United Kingdom, the United States and Brazil.[26] In contrast, there was no suggestion in the *Airbus* DPA that the company might face liability in other jurisdictions. Dame Victoria Sharp, the President of the Queen's Bench Division, emphasised the importance of 'international co-operation' from the court's perspective and pointed to *Innospec* in which the court noted that 'coherence in the level of financial penalties across different jurisdictions in cases of corporate wrongdoing is important so that forum shopping for the settlement of these kinds of cases is avoided'.[27]

In practice, global settlements can involve significant risks. An example is the prosecution in Greece of former employees of Johnson & Johnson and its subsidiary, DePuy International Limited (DePuy), which included the prosecution of one individual, Robert Dougall, notwithstanding his 2010 prosecution by the SFO and conviction and sentence.[28] Although Dougall was acquitted in the Greek proceedings, this case demonstrates that no settlement can confer an

23 *SFO v Amec Foster Wheeler Energy Limited* (Case No. U20210867) [2021].

24 Formerly known as Foster Wheeler Energy Limited, prior to its acquisition by Amec Foster Wheeler plc.

25 *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303.

26 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 68.

27 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, para. 92.

28 *R v. Dougall* [2010] EWCA Crim 1048.

© Law Business Research 2021

absolute guarantee against further proceedings in any jurisdiction – particularly not in jurisdictions where there is no limitation period for criminal offences (as in the United Kingdom, other than for summary offences). Dougall's prosecution must be contrasted with the outcome of the SFO's investigation of DePuy. The company was investigated by the SFO following a referral from the United States Department of Justice (DOJ), which, along with other domestic and foreign authorities, had been investigating Johnson & Johnson in relation to payments made by DePuy to intermediaries for the purpose of making corrupt payments to Greek medical professionals working in the Greek public health system.[29] The DOJ concluded a DPA with Johnson & Johnson in the United States as part of a global settlement over the unlawful conduct in Greece.

The SFO sought a CRO against DePuy rather than pursuing any criminal prosecution on the basis that such prosecution was prevented in the United Kingdom by the principle of double jeopardy. The former Director of the SFO, Sir David Green QC, took the view that the underlying purpose of the rule against double jeopardy is to stop a defendant from being prosecuted twice for the same offence in different jurisdictions: Johnson & Johnson's DPA with the DOJ had the legal character of a formally concluded prosecution and punished the same conduct in Greece that had been investigated by the SFO. That double jeopardy will be a bar to prosecution where a defendant has been convicted or acquitted by a foreign court on the same facts is uncontroversial,[30] but whether the conclusion of a DPA in the United States is equivalent to a formally concluded prosecution has not been tested in the courts. The SFO gave no detailed argument as to why it concluded that DePuy's prosecution in the United Kingdom was barred, and the application of the principles of double jeopardy in global settlements remains unclear.[31] The SFO's reasoning in relation to DePuy will also be problematic where as part of a global settlement it is seeking to agree its own DPA in the United Kingdom. If the SFO considers itself prevented by the rules of double jeopardy from pursuing criminal prosecution against a corporate that has agreed a DPA or other settlement with foreign authorities, then it may be prevented from agreeing a DPA under the statutory regime in the United Kingdom as prosecution may always follow a DPA if its terms are breached.[32]

Furthermore, no settlement can prevent private civil litigation, which could potentially be assisted or even encouraged by material generated in connection

29 'DePuy International Limited ordered to pay £4.829 million in Civil Recovery Order', press release dated 8 April 2011, SFO.

30 *Treacy v. DPP* [1971] AC 537 *per* Lord Diplock; see also the Decision of the Grand Chamber of the European Court of Justice in *Kossowski* (C-486/14, 29 June 2016), setting out the court's views on double jeopardy and its operation across EU Member States.

31 See the issue discussed in more detail in 'Deterring and Punishing Corporate Bribery: An evaluation of UK corporate plea agreements and civil recovery in overseas bribery cases', Transparency International UK policy paper published in May 2012, paras. 353 to 361.

32 Crime and Courts Act 2013 (UK), Schedule 17, para. 9.

© Law Business Research 2021

with the settled proceedings. However, settlement could make civil action less likely (or at least less likely to be successful), than were a contested criminal trial to take place, by reducing the volume of material entering into the public domain as compared to a full trial of the facts.

Whether a global settlement is worth pursuing is therefore likely to depend very much on the circumstances of each case. A key consideration will be the jurisdictions and agencies involved, and the particular form or forms of settlement contemplated.

Initial considerations 23.2

This chapter assumes that the corporate has already decided that a settlement is desirable in principle. This is not a straightforward exercise and will involve many of the considerations discussed in the other chapters in this book. This is likely to include a comparison of the likely cost of agreeing a settlement (and any agreed financial penalty) as against the likely cost of defending criminal proceedings and the probability of a conviction (and any penalty imposed). It will also include the reputational damage that contested criminal proceedings may have on a corporate. Corporates should also consider that a criminal conviction for certain economic and financial crimes may exclude them from competing for certain public contracts.[33]

Of course a corporate may also successfully argue that the authority should not institute any proceedings against it: prosecutors must be satisfied of the evidential basis of the prosecution as well as the public interest in prosecuting.[34] Many investigations in the United Kingdom result in no further action being taken against the subject of the investigation.

The attractiveness of a settlement is likely to vary considerably depending on the conduct under investigation and the investigating authorities involved. It is also likely to depend on the form of settlement available – for example, the advantages to a corporate of agreeing to a DPA in the United Kingdom may be very far removed from the advantages of agreeing to a DPA in the United States and *vice versa*. In some circumstances a settlement in the United Kingdom might not be an attractive prospect when considered in isolation, but the ability to secure a linked settlement with investigating authorities in another jurisdiction could tip the balance in favour of seeking a UK settlement as part of a global resolution.

Given that a settlement may not always be an obvious choice, the reasons for seeking to settle and the reasons for choosing a particular form of settlement should be clear before negotiations commence. The initial assessment of the corporate's eligibility for the kind of settlement sought must be realistic, based on the best available information about the conduct and a thorough

33 Public Contracts Regulations 2015 (UK); Public Contracts Directive, 2014/24/EU.

34 Crown Prosecution Service Guidance on Corporate Prosecutions, https://www.cps.gov.uk/legal-guidance/corporate-prosecutions.

© Law Business Research 2021

understanding of the attitude and approach adopted by the relevant authorities. The corporate will also need to be clear about the risks that settlement negotiations entail. In the event that the negotiations break down, the corporate might find itself in a worse position than it would have been in had it not entered into the negotiations in the first place. Finally, to demonstrate compliance with fiduciary obligations it will also be important to ensure that any decision makers have no personal interest in the outcome of settlement negotiations, as they would have if they were exposed to individual liability in connection with the conduct under investigation. This may be particularly complex in relation to small corporates where any decision-makers face individual liability for criminal conduct while simultaneously attracting liability to the corporate by acting as the directing mind and will.

23.2.1 Options for seeking a settlement

23.2.1.1 Civil recovery orders

A corporate could seek to persuade an investigating authority to dispose of an investigation by initiating civil recovery proceedings rather than a prosecution.

Civil recovery proceedings can be brought in the High Court by a number of UK enforcement agencies against property of a value in excess of £10,000 believed to have been obtained through unlawful conduct.[35] As a form of settling criminal proceedings a CRO has many features that could be helpful when a UK settlement is sought as one aspect of a global settlement. No prior UK conviction is required. The standard of proof is the civil one of the balance of probabilities. Judicial approval does not need to be sought before a claim can be brought, and the High Court's jurisdiction to make the order extends over assets located overseas; although it may in practice be tempered by the local law position on enforcement of orders that are not based on a conviction.

A CRO was for many years regarded as the best possible settlement outcome for corporates facing potential criminal proceedings in the United Kingdom, and an outcome that could plausibly be expected in a corporate self-reporting case. Two developments have impacted on this view.

First, under its current policy, the SFO will be less ready than it historically has been to dispose of an investigation by way of a CRO.[36] In part, this is a response to the OECD's criticisms of the UK's lack of commitment to

35 Part V, Proceeds of Crime Act 2002 (UK) (POCA). s.316 of POCA defines 'enforcement authority' in England and Wales as the National Crime Agency, the Director of Public Prosecutions or the Director of the SFO. The financial threshold of £10,000 is set in s.287, POCA and the Proceeds of Crime Act 2002 (Financial Threshold for Civil Recovery) Order 2003 (UK).

36 Guidance on Corporate self-reporting, issued by the SFO, revised in October 2012. Note also the position in Scotland where the Crown Office and Procurator Fiscal Service issued guidance in June 2017 stating that prosecutors may consider civil settlement for corporates that self-report offences under the Bribery Act 2010.

© Law Business Research 2021

combating bribery of foreign public officials.[37] In the event that the SFO were to agree to a CRO, its terms will now be published in full, which removes some of the historically perceived benefit of this form of settlement.[38]

Secondly, the SFO has demonstrated that civil recovery proceedings and criminal proceedings are not necessarily mutually exclusive provided that the conduct can be divided. In conjunction with the conviction of Bruce Hall in 2012 and the making of a confiscation order and compensation order against him, the SFO brought civil recovery proceedings in respect of conduct falling outside the scope of the indictment because UK jurisdiction did not arise.[39] This has to be considered, however, against the background of the criticism by Thomas LJ in *Innospec* of the use of a CRO in addition to trial on indictment; Thomas LJ concluded that where the facts and public interest determined that a prosecution was appropriate, the use of the civil jurisdiction was consequently inappropriate. In particular, the judge deprecated the possibility of matters arising in the same case coming within the jurisdiction of two separate judges from two separate courts. In contrast, the use of a CRO for DePuy was less problematic as the corporate was not the subject of an indictment.

See Section 23.1

Deferred prosecution agreements 23.2.1.2

A DPA may be regarded as the half-way house between a negotiated plea agreement and a CRO. A DPA is only available in limited circumstances; the power to apply to the courts for a DPA rests solely with the prosecutor,[40] and the DPA provisions reserve to the prosecutor (currently only the SFO or the Crown Prosecution Service (CPS)) the right to extend any invitation to enter into DPA negotiations. In addition, as was identified by the former Director of the SFO,[41] the high threshold for corporate criminal liability under English law reduces the incentive for corporates to enter into a DPA at all. To date, none of the 12 DPAs secured in the United Kingdom appears to have faced any difficult application of corporate criminal liability: *Standard Bank plc*, *Airbus* and *Airline Services Limited*[42] concerned the strict liability offence of failing to prevent bribery under section 7 of the Bribery Act 2010; *XYZ Ltd (Sarclad)* applied to a small company in which the directing mind and will was

37 'Report on the Application of the Convention on Combating of Foreign Public Officials in International Business Transactions and the 1997 Recommendations on Combating Bribery in International Business Transactions', approved and adopted by the OECD Working Group on Bribery in International Business Transactions on 16 October 2008.

38 Statement of David Green QC, then Director of the SFO, 17 April 2013. See, e.g., 'Oxford Publishing Ltd to pay almost £1.9 million as settlement after admitting unlawful conduct in its East African operations', press release dated 3 July 2012, SFO.

39 'Bruce Hall sentenced to 16 months in prison', press release dated 22 July 2014, SFO.

40 See Crime and Courts Act 2013 (UK), Schedule 17, para. 8.

41 Sir David Green QC, then Director of the SFO, speech given at Pinsent Masons and Legal Week Regulatory Reform and Enforcement Conference, 24 October 2013.

42 *Director of the SFO v. Airline Services Limited* (Case No. U20201913) [2020].

© Law Business Research 2021

easily identified; *Rolls-Royce, GSL* and *AFWEL* concerned the strict liability offence of failing to prevent bribery as well as substantive offences of bribery and corruption involving, on the facts as admitted by those entities for the purposes of the DPA, controlling minds of the company; and in *Tesco Stores Limited*,[43] *Serco Geografix Limited*[44] and *G4S C&J*, the alleged offences were said to have been committed by individuals who the parties accepted constituted the directing mind and will of the respective companies.[45] The DPA Code of Practice provides little guidance as to what extent a corporate entity can introduce the possibility of a DPA into any discussions it may hold with the SFO, but it does outline the factors the SFO will consider when inviting a corporate to enter into a DPA, the process of being invited into DPA negotiations and a framework for once negotiations have begun.[46]

In theory, a DPA should be an attractive form of settlement as the corporate avoids prosecution, escaping some of the stigma and adverse publicity necessarily associated with any criminal trial and, if successful, a conviction. A corporate will have the opportunity to make representations on and to influence the terms of the settlement that is made public, and there will be no mandatory debarment from public contracts. Importantly, a DPA may be part of a global resolution that may be in the overall commercial interests of the corporate.

The corporate is nevertheless the subject of criminal proceedings that are suspended. The offences alleged to have been committed are particularised in an indictment, and further detailed in the statement of facts accompanying the DPA. The terms of the DPA will include not only a financial penalty but may also include disgorgement of profits and compensation payments. Unlike a criminal sentence, a DPA may extend to requiring the corporate to submit to a compliance monitor for a specified period.[47]

The terms of the DPA may require the corporate to disgorge the gross profit made as a result of the criminal conduct.[48] The DPA may also impose a financial penalty,[49] which must be broadly comparable to the fine that a court would have imposed on conviction and is accordingly assessed by reference to the relevant Sentencing Guideline for fraud, bribery and money laundering

43 *SFO v. Tesco Stores Limited* (Case No. U20170287) [2017] 4 WLUK 558.

44 *SFO v. Serco Geografix Limited* [2019] 7 WLUK 45, [2019] Lloyd's Rep FC 518 (*Serco Geografix Limited*).

45 The 11th and 12th DPAs, announced by the SFO on 20 July 2021, concern two UK-based companies charged with bribery offences contrary to ss.1 and 7 Bribery Act 2010. Both DPAs share a common statement of facts but this statement remains under reporting restrictions and the identities of the relevant companies have not yet been released.

46 Deferred Prosecution Agreement Code of Practice, issued by the Director of Public Prosecutions and Director of the SFO (DPA Code of Practice), paras. 2.1 and 3.

47 Crime and Courts Act 2013 (UK), Schedule 17.

48 ibid., para. 5(3)(d).

49 ibid., para. 5(3)(a).

© Law Business Research 2021

offences (Sentencing Guideline).[50] Where the corporate has limited means and ability to meet these financial obligations, the court may nevertheless approve a penalty that would render the corporate insolvent where it would be in the interests of justice to do so.[51] Among other things, the court will consider the impact of any financial penalty on the corporate's staff, service users, customers and the local economy. In *XYZ Ltd (Sarclad)*, the corporate's parent agreed to provide financial support to Sarclad by returning almost £2 million from dividends received for Sarclad to pay towards disgorgement.[52] The court made clear that the innocent parent was under no contractual or legal obligation to contribute towards the financial penalty imposed on its subsidiary for the criminal conduct.[53] However, the court did point out that the parent had received £6 million in dividend payments since acquiring Sarclad. As in *Sarclad*, the parent company of AFWEL John Wood Group plc (Wood), which had guaranteed the obligations of its subsidiary under the DPA, was also determined to be an innocent party in respect of the proceedings[54] because the alleged wrongdoing committed by AFWEL had occurred even before Wood's predecessor (Amec Foster Wheeler plc) acquired the company. Wood's 'twice removed' distance from the alleged wrongdoing was a critical factor in Mr Justice Edis's decision that a DPA was in the interests of justice; if any of the individuals involved in the alleged wrongdoing had still been involved in AFWEL, a DPA would not have been deemed appropriate.[55] Further, Wood did not seek a reduction in the price it paid for AFWEL to account for the contingent liabilities that might have arisen from the SFO's investigation into the company, and so was able to benefit from a 50 per cent reduction in the financial penalty it was required to pay pursuant to the DPA (which still amounted to almost £50 million not including disgorgements of approximately £48 million). If Wood had sought a reduction in the purchase price, it would have been deemed to have benefited inappropriately from the wrongdoing of AFWEL and a reduction would likely not have been granted.[56] Mr Justice Davis relied on the reasoning in *XYZ Ltd (Sarclad)* when he made no order as to financial penalty nor the SFO's costs in *GSL* recognising that a disgorgement of £2.07 million in gross profit was all the company could sensibly be expected to pay.[57] Unlike the other DPAs in which a financial penalty was required to be paid immediately or a clear timetable of payments was iden-

50 Fraud, bribery and money laundering offences: Definitive guideline, issued by the Sentencing Council, in force from 1 October 2014.

51 *XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509, paras. 23, 24.

52 ibid., para. 22.

53 ibid., para. 21.

54 *SFO v. Amec Foster Wheeler Energy Limited* (Case No. U20210867) [2021], para. 30

55 ibid., para. 29.

56 ibid., para. 30.

57 *Güralp Systems Ltd* (Case No. U20190840) [2019], paras. 42–43.

© Law Business Research 2021

tified, GSL's only requirement regarding the disgorgement of profits was to make the payment by the fifth anniversary of the DPA.[58]

In *Rolls-Royce*, the total financial orders (including those imposed in the United States and Brazil) amounted to over £650 million even after a 50 per cent reduction of the UK element of the financial penalty in recognition of Rolls-Royce's 'extraordinary' co-operation.[59] The Court was satisfied that this figure was sufficient to bring home to both management and shareholders the need to operate within the law without being so high as to put Rolls-Royce out of business, which would have been inappropriate in the circumstances.[60]

In *Serco Geografix Limited*, the company was ordered to pay a financial penalty of £19.2 million and the SFO's investigative costs of £3,723,679. The company would also have been required to pay compensation of £12.8 million, but this was fully offset by payments made pursuant to Serco Limited's 2013 settlement agreement with the UK Ministry of Justice.[61] Similarly, in *G4S C&J*, the company was ordered to pay a financial penalty of £38.5 million and the SFO's costs of £5.95 million, but no compensation or disgorgement of profits since the court took into account the settlement which had been reached in 2014 under which G4S C&J agreed to pay £121.2 million to settle the Ministry of Justice's claims against the company.[62]

In settling with the French National Financial Prosecutor (PNF), the SFO, the US DOJ and Department of State (DOS), Airbus faced a global financial sanction in excess of €3.5 billion, of which close to €1 billion was paid to the SFO. This comprised the disgorgement of profits of €585.9 million, the SFO's costs of €6.9 million and a financial penalty of €398 million. As noted by Sharp P in her judgment, this was the largest UK DPA financial settlement to date and greater than the combined total of all previous financial settlements under UK DPAs.[63]

The process of negotiating a DPA could itself deter a corporate from seeking this sort of settlement. It is lengthy and uncertain, as any agreement reached with the relevant prosecuting authority is ultimately conditional on judicial approval. It is accompanied by potentially as great a degree of public scrutiny as may be attracted by contested criminal proceedings. The provision of false, misleading or incomplete information to the relevant prosecuting authority could amount to an offence,[64] and it can be extremely challenging

58 ibid., para. 40.

59 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 128.

60 ibid., para. 127.

61 *Serco Geografix Limited* [2019] 7 WLUK 45, [2019] Lloyd's Rep FC 518, para. 37.

62 *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, paras. 22 and 35–36.

63 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, paras. 1 and 2.

64 For example, for attempting to pervert the course of justice, contrary to the common law. Prosecution of the offence that is the subject of the DPA can also follow if the organisation provided information to the SFO that it knew or ought to have known was inaccurate, misleading or incomplete, see *XYZ Ltd (Sarclad)* and *Rolls-Royce*.

© Law Business Research 2021

for a corporate, and the relevant individual within the management structure, to certify that the material provided to the investigating agency is complete.

The DPA may become a more attractive option for corporates if there is more flexibility on the terms imposed and if higher discounts to financial penalties or sentences continue to be applied. With respect to increased discounts, the DOJ's enhancements to its Pilot Program could be of interest to the SFO. In November 2017, the DOJ announced that the Pilot Program it launched in 2016 to encourage companies to self-report potential violations of the Foreign Corrupt Practices Act (FCPA) would be made permanent and incorporated into the United States Attorneys' Manual (now known as the Justice Manual), subject to some amendments.[65] Under the revised FCPA Corporate Enforcement Policy, where a company 'satisfies' the DOJ's standards of 'voluntarily self-disclosing, fully co-operating and 'timely and appropriately remediating', there will be a 'presumption' that the government will resolve the matter with a declination – unless there are aggravating circumstances (for example, recidivism). However, even where circumstances 'compel' a criminal enforcement action, the DOJ will recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines fine range for self-reporting companies, except in the case of a criminal recidivist. Finally, to be eligible for leniency under the FCPA Corporate Enforcement Policy, a company must pay all disgorgement, forfeiture, and restitution resulting from the misconduct at issue.

In the DPA reached with XYZ Ltd (Sarclad), the court stated that a discount of 50 per cent to the financial penalty that would have been imposed[66] was appropriate, given that the corporate had self-reported and admitted the criminal conduct far in advance of the earliest possible opportunity that would have applied after a criminal charge.[67] This sizeable reduction was not based on an application of the Sentencing Guideline or the DPA statutory provisions themselves.

Even more surprising (at first glance) was the application of a 50 per cent discount to the financial penalty in *Rolls-Royce*, where the corporate did not make the initial self-report.[68] The initial report of suspicions of criminality in the corporate's civil business in Asia came from public internet postings and precipitated the SFO's investigation; however, this led to an immediate and extensive investigation by the corporate during which it made a number of voluntary reports to the SFO in respect of other business lines in multiple

65 'Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act' Press release, 29 November 2017.

66 In fact, as the judge made clear, the question of a penalty was 'academic because, given the amount disgorged, whatever multiplier is chosen and however substantial the discounts, the result is a figure which Sarclad simply cannot pay and which would result in its insolvency', para. 55.

67 *XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 211, [2016] Lloyd's Rep FC 517.

68 *Rolls-Royce* (Case No. U20170036) [2017] [2017] 1 WLUK 189, Lloyd's Rep FC 249, para. 123.

© Law Business Research 2021

jurisdictions.[69] Rolls-Royce's co-operation with the SFO and other authorities was said to be 'extraordinary'.[70] Rolls-Royce took a number of steps in addition to the extensive investigation and voluntary reports to authorities: it reviewed relationships with intermediaries, agents, advisers and consultants; provided over 30 million documents in electronic and hard copy form (Rolls-Royce agreed to the use of digital methods to identify privilege issues in the material and the use of independent counsel in relation to the privilege review); allowed the SFO to interview witnesses first and waived privilege over its own internal interview memoranda; provided material to the SFO voluntarily (without need for recourse to compulsory powers); consulted with the SFO in respect of media coverage; provided all financial data sought by the SFO and co-operated with financial assessments undertaken; and sought the SFO's permission before winding up companies that may have been implicated in the SFO's investigation.

The SFO submitted that in the particular circumstances of the case, the Court should not distinguish between the corporate's assistance and that of those who have self-reported from the outset. This was accepted on the basis that what Rolls-Royce reported was far more extensive and of a different order than might have been exposed without its co-operation.[71] The Court was satisfied that, from the moment of the initial question from the SFO prompted by the public postings on the internet, Rolls-Royce could not have done more to expose its own misconduct. Self-reporting was said in the judgment to be a core purpose of DPAs, and the weight this attracts depends on the totality of the information provided; it seems that the measures that Rolls-Royce took to unearth and report the extent of the criminality made up for the absence of an initial self-report.[72]

The decision in *Serco Geografix Limited* revisited the issue of self-reporting and co-operation. In his concluding comments, Mr Justice Davis noted that any cynicism about the process by which a corporate entity can take advantage of a DPA 'is not well-founded' and that approval will only be given where there is the 'clearest possible demonstration of integrity' on the part of the relevant company, which will require self-reporting, full co-operation with the investigation, a willingness to learn lessons and acceptance of an appropriate penalty. He added that a willingness to learn lessons must be shown via 'real, substantial and continuing remedial measures'.[73] The court proceeded to apply a 50 per cent discount and referred to the fact that in all but one of the earlier instances of approval of DPAs, the financial penalty has been discounted by

69 ibid., para. 17.

70 ibid., paras. 16 to 20 and 121.

71 ibid., para. 22.

72 ibid., para. 38.

73 *Serco Geografix Limited* [2019] 7 WLUK 45 [2019] Lloyd's Rep FC 518, para. 47.

© Law Business Research 2021

50 per cent rather than one third. This was found to 'encourage corporate responsibility in terms of early reporting of criminal conduct'.[74]

In *Airbus*, Sharp P adopted a similar approach to Leveson P in *Rolls-Royce* and took 'self-reporting' to encompass all subsequent self-reports that were of a high-quality and brought significant wrongdoing to light.[75] Airbus was found to have co-operated with the SFO 'to the fullest extent possible' despite it getting off to a 'slow start'.[76] One particularly notable part of Airbus' co-operation included the 'unprecedented step' for non-UK companies to accept the SFO's jurisdiction in respect of the reporting of conduct which had taken place exclusively overseas.[77] This serves as a useful reminder to non-UK parent companies that their management of UK-incorporated subsidiaries may make the parent subject to the UK Bribery Act 2010, even in respect of conduct which is unrelated to the United Kingdom.

Sharp P acknowledged that the 'true catalyst' for the self-report to the SFO was the dialogue with UK Export Finance (UKEF), but noted that Airbus had identified 'red flags' to UKEF when Airbus knew that UKEF considered itself obliged to report corruption.[78] The result is a growing body of cases suggesting that a DPA may be available in the absence of an initial self-report, if there is sufficiently extensive subsequent co-operation and ongoing reporting of 'new' misconduct. Further, a report to a body that it is known will pass information to the SFO may attract some 'co-operation credit'.

There is a clear view among practitioners that the incentives to enter into a DPA, in particular the apparent maximum discount on penalty, embedded within the statutory scheme,[79] of one-third (the same as for an early guilty plea) is insufficient and fails to recognise the positive factors in the conduct of the corporate that will have led to the offer of a DPA in the first place. This view appears to have been accepted by the SFO and the judiciary, as a 50 per cent reduction has been applied on each occasion since the *Standard Bank plc* DPA except for *G4S C&J*, who was given a 40 per cent discount on the basis that the company's co-operation could not, unlike the other DPAs, be said to be 'extraordinary or otherwise exemplary'. In this case, Mr Justice Davis noted that G4S C&J was entitled to more than the minimum 33 per cent discount available under a DPA, but it was not entitled to the full 50 per cent discount as its cooperation had been initially 'less than full'.[80]

74 ibid., para. 37.

75 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, para. 68.

76 ibid., paras. 69 and 70.

77 ibid., paras. 72 and 74.

78 ibid., para. 71.

79 Crown and Courts Act 2013 (UK), Schedule 17, para. 5(4).

80 *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, para. 40.

© Law Business Research 2021

23.2.1.3 Negotiated plea agreements

A plea agreement can be negotiated with the prosecutor at any stage after indictment, up to the conclusion of the trial. It may be preceded by advance representations on charge, which a prosecutor is under no obligation to consider but may do so at his or her discretion. Both advance representations and plea agreements could potentially reduce the scope of the conduct charged, or even determine the nature of the offence charged; as seen in *BAE Systems*,[81] where the corporate had been investigated for overseas corruption but pleaded guilty to knowingly procuring the failure of its subsidiary, British Aerospace Defence Systems Ltd (BADS), to comply with the provisions of section 221 of the Companies Act 1985, and thereby aiding and abetting, counselling and procuring the commission of the offence contrary to section 225 of the Companies Act, by the officers of BADS.[82] In *BAE Systems*, Mr Justice Bean was critical of the restriction on the scope of the conduct in the settlement reached between the corporate and the SFO, and in light of these criticisms prosecuting authorities may in future be less willing to minimise the conduct in negotiated plea agreements.[83] Mr Justice Bean made clear that in cases involving negotiated plea agreements the judge will not be bound by the agreement between the prosecution and the defence, and the prosecution's view on the proposed basis of the plea is deemed to be conditional on the judge's acceptance of the basis of the plea.[84] The judge made clear that the involvement of the criminal courts precludes the passing of a sentence on an artificial basis. While Mr Justice Bean accepted the basis of the sentence in *BAE Systems*, this may not always be the case.[85]

The judge also expressed surprise that the SFO had committed to a blanket indemnity against investigations or prosecutions of any member of the BAE Systems group for past conduct whether disclosed or otherwise.[86]

However, even if the charges remain unchanged, a guilty plea at the earliest possible stage makes the corporate eligible for a reduction of up to one-third off the sentence that would otherwise have been imposed on conviction.[87]

---

81 *R v. BAE Systems plc* [2010] EW Misc 16 (CC) (*BAE Systems*).

82 *Corruption and Misuse of Public Office* (2nd Ed.), Collin Nichols QC, Timothy Daniel, Alan Bacarese and John Hatchard, at p. 39.

83 *BAE Systems*, para. 13.

84 *R v. Underwood* [2004] EWCA Crim 2256; BAE Systems, para. 13.

85 The principles underlying this reasoning are also reflected in the statutory regime for DPAs, which must be approved by a judge as being in the interests of justice; see further Section 23.2.1.2.

86 *BAE Systems*, para. 5.

87 Reduction in Sentence for a Guilty Plea: Definitive guideline, Sentencing Council, 23 July 2007, para. 4.2 (for cases where the first hearing was before 1 June 2017); Reduction in Sentence for a Guilty Plea: Definitive Guideline, Sentencing Council, 7 March 2017, para. D1 (for cases where the first hearing was after 1 June 2017).

© Law Business Research 2021

UK prosecutors will invariably be open to negotiations on plea. The prosecution and the defence are in all cases required to resolve issues and agree evidence wherever possible prior to trial.[88] The prosecutor must, however, have regard to any applicable restraints on the exercise of discretion, including the Witness Charter and the Code of Practice for Victims of Crime.[89] In accordance with the Code for Crown Prosecutors, prosecutors will also need to ensure that the plea reflects the seriousness and extent of the offending.[90] The Attorney General's Guidelines to the legal profession state that prosecutors must not agree to a basis of plea that is misleading, untrue or illogical or insupportable.[91] Where a case involves multiple defendants, the bases of plea must be factually consistent. Trial judges may ultimately, of their own motion, disregard the agreement and direct a 'Newton' hearing to establish the relevant facts.[92]

Just as the decision on whether to accept a proposed basis of plea is ultimately one for the trial court, it is similarly for the sentencing court to impose the sentence on conviction. In cases of serious and complex fraud the Attorney General's Guidelines permit the prosecution and defence to present a joint written submission to the court on sentence but this is not binding on the court. In *R v. Dougall*, the court declined to impose the SFO's suggested suspended sentence on an assisting offender, although the custodial sentence that the court did impose was overturned on appeal. The Court of Appeal criticised the SFO for adopting a role that was more akin to that of the defence. The courts in *BAE Systems* and in *Innospec* felt compelled to accept the suggested sentences because they formed part of a global settlement that the corporate entity had been invited to accept (and because of the corporate's limited financial resources in *Innospec*), but Thomas LJ in *Innospec* warned that this approach would not be repeated in the future.

The attractiveness of a plea agreement to a corporate will depend largely on the weight of the prosecution evidence, including the existence of any co-operating co-offenders under the 'offender assistance' provisions set out in sections 71 to 75 of the Serious Organised Crime and Police Act 2005. In particular, the corporate's willingness to plead is likely to reflect an assessment that the prosecutor would be able to establish corporate criminal liability. As mentioned in the introduction to this chapter, guilty pleas by corporates are more likely to be forthcoming for offences where the identification principle does not apply or liability is strict, or both, or where the corporate is small and

88 Criminal Procedure Rules 2015 (UK), Rule 3.3.

89 The Witness Charter, issued by the Ministry of Justice, December 2013; Code of Practice for Victims of Crime, issued by the Ministry of Justice, October 2015, last updated 8 October 2018.

90 The Code for Crown Prosecutors, October 2018, para. 9.

91 See 'Plea discussions in cases of serious or complex fraud', 29 November 2012; and 'The acceptance of pleas and the prosecutor's role in the sentencing exercise', 30 November 2012, Attorney General's Office.

92 Consolidated Criminal Practice Direction, para. IV.45.10.

© Law Business Research 2021

lines of responsibility are clear; by contrast, the prosecution might in other cases struggle to identify culpable senior management.

The size of the likely penalty will also be a factor when the corporate is considering whether to plead. There is an established procedure in place by which a defendant in Crown Court proceedings can seek a binding indication from the trial judge of what sentence would be imposed on a guilty plea (*Goodyear* indication).[93] That Guideline may have similarly increased the attractiveness of plea agreements for corporates, not only by making the likely sentence more predictable at an even earlier (pretrial) stage but also by increasing the risk of higher penalties being imposed than has historically been the case and thereby incentivising an early, negotiated settlement.

The downsides of a plea agreement include the inability to contest the charges in a public forum, and loss of the opportunity of an acquittal. The advantages of a plea agreement also decline rapidly with time once a trial is under way.

There are also risks arising from plea negotiations. The Attorney General's Guidelines state that the prosecutor may not rely on the defendant's participation in plea negotiations or on any information disclosed during those negotiations as evidence against the defendant in the event that the negotiations fail but a signed plea agreement can be relied on as confession evidence against the defendant. A prosecutor would normally be free to rely on any evidence gathered as a result of enquiries made on the back of information disclosed in the course of the negotiations, and information provided by the defendant in connection with the negotiations could normally be relied on both in related prosecutions of other defendants and in a prosecution of the defendant for another offence. In addition, the prosecutor might be obliged to disclose material relevant to the negotiations to a co-defendant.

23.2.2 Strategic considerations when seeking a settlement in the United Kingdom

Once a corporate has decided in principle to seek to settle criminal proceedings in the United Kingdom, the objective will be to achieve the desired form of settlement as effectively as possible, avoiding or minimising, to the fullest extent possible, adverse consequences. This section will discuss common strategic considerations that are likely to arise at the outset and during the early stages of settlement negotiations.

23.2.2.1 Timing of settlement

A preliminary strategic consideration will be the point at which to approach the relevant authority. On the one hand, a successful outcome is more likely the earlier an approach is made. The financial and reputational costs to a corporate

93 In accordance with *R v. Goodyear* [2005] EWCA Crim 888 and by reference to the Sentencing Guideline.

© Law Business Research 2021

of being a subject of a criminal investigation and prosecution will increase incrementally and early self-reporting is an important factor in determining whether a DPA will be offered. Clearly, however, the corporate needs to have sufficient knowledge about the conduct it proposes to report.

A corporate may self-report the conduct in question or otherwise bring it to the attention of the relevant authorities, for example, pursuant to money laundering reporting obligations or, for listed corporations, obligations to disclose information to the market. The SFO published guidance on self-reporting in 2012[94] and, in 2019, published internal guidance outlining what it considers to be good practice with respect to co-operation by a company under investigation.[95]

In all other cases the determining factor is likely to be the type of settlement sought. Where the favoured outcome is a CRO, the driver will be to reach agreement on this form of alternative disposal before any steps are taken to initiate criminal proceedings. If the preferred form of settlement is a DPA, the timing of the settlement will be dictated by the DPA Code of Practice, but again will involve negotiations with the authority before the commencement of criminal proceedings. A settlement could be reached at any of the following points in time.

See Section 23.2.1.2

Before major production of documents

A corporate must balance the need to understand any potential criminal liability it faces with the benefit of making an early report to an authority. As stated above, corporates should establish sufficient knowledge of the circumstances before deciding to seek a settlement. Once that decision has been made, it is unlikely that an agency in the United Kingdom will be prepared to reach a settlement agreement without receiving all relevant documentation and undertaking some form of investigation. Once in the hands of the authorities, any material provided could be used against the corporate and individuals. In addition, such material can be provided to other domestic and international agencies and may ultimately be disclosed in any related civil proceedings. It also has to be assumed that documents provided to investigating agencies may ultimately end up in the public domain.

Before witness testimony

To the extent that corporates record any interviews they conduct, UK authorities are likely to want access to these first accounts, which may raise issues of legal professional privilege. The Court of Appeal's judgment in *Director of*

94 Guidance on Corporate self-reporting, issued by the SFO, revised in October 2012. See also the Guidance on corporate prosecutions issued by the Director of Public Prosecutions, the Director of the SFO and the Director of the Revenue and Customs Prosecutions Office, issued in 2009–2010.

95 Corporate Co-operation Guidance, issued by the SFO, 6 August 2019.

© Law Business Research 2021

the SFO v. ENRC[96] has brought some much-needed clarity to this area of the law, following two conflicting first-instance decisions of the High Court of England and Wales.[97]

The Court of Appeal in *ENRC* disagreed with the High Court's strict approach to whether notes of interviews attract litigation privilege, finding that uncertainty over whether criminal proceedings were likely would not in itself prevent litigation from being in reasonable contemplation, and that the whole subtext of the relationship between the relevant company and the authorities was important. In this case, the court found that the relationship between ENRC and the SFO meant that there was a possibility, if not a likelihood, of prosecution if the self-reporting process did not result in a settlement. The court also said that where the SFO made explicitly clear in its communications to the company that there was the prospect of a criminal prosecution, and external legal advisers were engaged to deal with that possibility, there was a clear ground for contending that criminal prosecution, and therefore litigation, was in reasonable contemplation at the time the interview notes were prepared.

The Court of Appeal also found that the need to investigate the existence of alleged corruption was a subset of defending the litigation, and hence that notes made in interviews during the investigation stage were made for the dominant purpose of litigation.

See Chapter 36 on privilege

This decision underlines the importance of obtaining advice when corporates need to conduct and create records of interviews during the fact-finding stage of an investigation, and before a prosecution decision is made by the authorities, to understand the alleged facts and any potential liability. Ordinarily, the SFO will still conduct interviews as part of its investigations following a self-report, even where there have already been interviews by the corporate. Nevertheless, the authorities may in some cases expect a corporate that wishes to obtain credit for co-operating, to waive privilege over certain documents that have been prepared during the investigation stage, including any reports that have been prepared for the internal investigation,[98] for the dominant purpose of engaging in settlement negotiations with the authorities. The SFO's internal guidance on corporate co-operation[99] states that in addition to witness accounts, companies seeking credit for co-operating should provide any recording, notes and transcripts of interviews and identify a witness competent to speak to the contents of each interview.

Legal advice on the limitations that should be explicitly placed on any privilege waiver a corporate proposes to provide is an essential safeguard. As a recent example, in 2016 Barclays Plc and Barclays Bank Plc (Barclays) gave

96 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006.

97 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB) and *Bilta (UK) Ltd & Ors. v. Royal Bank of Scotland and Mercuria Energy Europe Trading Ltd* [2017] EWHC 3535 (Ch.).

98 Guidance regarding DPAs in a new chapter of the SFO's Operational Handbook, published by the SFO in October 2020.

99 Corporate Co-operation Guidance, issued by the SFO, 6 August 2019.

© Law Business Research 2021

a limited waiver to the SFO during its investigation into the conduct of the bank and certain executives during capital raisings in 2008, in respect of which legal advice had been taken.[100] In the civil proceedings that followed immediately after the criminal trial of certain Barclays executives, *PCP Capital Partners LLP v. Barclays Bank Plc*,[101] the bank sought to withhold privilege in respect of legal communications that had not been used in the criminal trial and had not therefore lost their privileged status as a result. However, in deploying the lawyers' advice in the civil proceedings to support its case on the merits, the bank was found by the High Court to have effectively waived privilege in all communications with its lawyers relating to two particular transactions. This decision was made despite the bank limiting reliance to documents that had already lost their confidentiality having been used in the criminal proceedings shortly before the civil case.

Before indictment

In most cases, corporates will be seeking to settle before indictment. As discussed above, settlement negotiations may provide an opportunity to influence the content and timing of the indictment.

Before trial

A settlement at the early stages of criminal proceedings may help to mitigate reputational damage by reducing the amount of material made available to the authorities and, through them, potentially becoming available in the public domain or to other overseas agencies.

There may yet be benefits of settling after the commencement of trial. Although disclosure obligations will have been complied with and material may have been referred to in open court (thereby becoming accessible to the public), by avoiding witness testimony the corporate may minimise the risk of further reputational and other costs as a result of adverse prosecution testimony or unpredictable defence witnesses. Settling before conviction could potentially also serve a public relations objective in presenting the corporate publicly as being somewhat co-operative (despite initially contesting the proceedings).

Ability to secure a global settlement 23.2.2.2

An early settlement of UK criminal proceedings may also increase the prospects of concluding a global settlement. In the global settlement scenario, timing is likely to be primarily driven by the authority 'leading' the settlement negotiations. As press reports suggested in relation to the LIBOR investigation, there

100 *PCP Capital Partners LLP and another v. Barclays Bank plc* [2020] EWHC 1393 (Comm), para. 10.

101 ibid.

© Law Business Research 2021

can be a 'race' among investigating authorities to charge defendants as a means of securing jurisdiction.[102]

Where a number of authorities may be investigating or have an interest in investigating the conduct, the potential for conflicts of jurisdiction to arise should be addressed by communications between prosecutors pursuant to multilateral and bilateral agreements such as the Eurojust guidelines for deciding which jurisdiction should prosecute and the Agreement for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States.[103] Prosecutors engaged in plea negotiations in serious and complex fraud cases are directed by the Attorney General's Guidelines to liaise with any counterparts known to have an interest in the defendant, in accordance with the Prosecutors' Convention and any other relevant agreement or guidance.[104] However, these arrangements would not be enforceable by corporates who find themselves adversely affected by any departures from their terms; in any event, such agreements do not tend to address settlements.

In practice, constructive global settlement discussions require a high level of communication between the investigating agencies involved and also between the lawyers acting for the corporate and those investigating agencies. By way of example, in *Standard Bank plc* there was clearly a high level of communication between the SFO and the DOJ (as well as between the bank's lawyers and both the SFO and the DOJ), which ultimately resulted in the DOJ confirming in writing in advance of the UK settlement that in view of the terms of the proposed settlement it did not propose to continue its own investigation.

The SEC, on the other hand, decided to continue with its own investigation into the civil (as opposed to criminal) consequences of the alleged conduct, which resulted in a separate settlement with the bank. Although the SEC's investigation related to separate issues, the bank completed its settlement with the SEC very shortly before the final DPA hearing in the United Kingdom and the settlement was announced on the same day. Coordinating the timing of the settlement so that it was announced at the same time was clearly in the bank's interests, as it ensured that the UK and US investigations into the conduct were resolved simultaneously, with the bank able then to draw a line under the events and focus on the future.

Similarly, in *Rolls-Royce* it was clear that substantial discussions had taken place between the SFO, the DOJ and the Brazilian public prosecutor to ensure a coordinated global resolution of the relevant conduct; indeed, its DPA with

102 See, e.g., 'US DoJ issues arrest warrant for Briton in Libor probe', Caroline Binham, 6 February 2015, *Financial Times*.

103 Annex A – Eurojust Guidelines – 'Which Jurisdiction Should Prosecute?', Annual Report 2003, issued by Eurojust (revised in 2016); Agreement for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States of America, January 2007.

104 Prosecutors' Convention 2009 (updated in September 2019), agreed by a number of UK prosecuting authorities including, *inter alia*, the SFO, the FCA, the Crown Prosecution Service and the Attorney General's Office.

© Law Business Research 2021

the DOJ was fully disclosed in the UK DPA proceedings,[105] and the DPA hearing in the United Kingdom was brought forward for reasons linked to the change in administration in the United States in January 2017.[106] Rolls-Royce announced settlements with those authorities in parallel with its DPA with the SFO. The corporate was apparently able to coordinate between prosecuting authorities such that it was prosecuted for different conduct in different jurisdictions;[107] it was also given US$25 million credit by the DOJ for fines paid in Brazil in relation to conduct that was overlapping between its DPA in the United States and its leniency agreement in Brazil.[108]

In *Airbus*, the DPA represented the conclusion of the SFO's joint investigation with the PNF into the company and the investigation conducted by the DOJ and DOS in parallel. Each prosecuting authority took responsibility for a number of geographical areas in which Airbus operated or customers of Airbus and simultaneously entered into their own form of resolution with the company: a DPA, judicial public interest agreement (CJIP), and a consent agreement. A joint investigation team agreement, which is novel in the DPA context, was entered into between the SFO and PNF.[109] It seems that one reason for this was to ensure access to relevant information that the SFO would otherwise have been unable to receive because of the French Blocking Statute prohibiting certain disclosures of information by French persons in foreign proceedings.[110] The PNF also took primacy over a number of aspects of the case.[111]

It is important to keep in mind when negotiating simultaneous settlements with multiple authorities and regulators (both at home and abroad) that the subject ensures that the published findings in each investigation concluded by a negotiated settlement are consistent, as authorities may have an incomplete understanding, or different interpretation, of the facts.

Written submissions to UK prosecuting authorities 23.2.3

One important risk that settlement negotiations pose for corporates is that the material generated will be relied on in the event that the negotiations break down; whether by the recipient authority or by third parties. Even if settlement negotiations will attract confidentiality to varying degrees, there will always be a number of avenues through which material provided to the authorities may be made available to other authorities and to third parties.

105 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 5.

106 ibid., paras. 10 and 12.

107 ibid. 17 January 2017, para. 5.

108 US Department of Justice, press release, 'Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case' (17 January 2017).

109 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, paras. 2 and 34.

110 ibid., para. 34.

111 ibid., paras. 34 and 92.

© Law Business Research 2021

The extent to which settlement negotiations will generate material, and the extent to which such material may be protected from onwards disclosure, will depend on the form of settlement in question. Written submissions made to a prosecutor in the course of negotiating a plea agreement are confidential and will only be made available to third parties where it can be shown that the prosecutor's obligation to preserve confidentiality is outweighed by a countervailing interest.[112] In DPA negotiations, both the form and content of documents are governed by statute and are not negotiable. These documents will include the draft statement of facts and the terms of the proposed DPA, as well as the preliminary application to the court.[113] The prosecutor will require these documents to be agreed before the application to the court can proceed. They will also include any submissions contained in related correspondence with the prosecutor, as well as minutes of any meetings between the corporate and the prosecuting authority.

23.2.4 Oral presentations to UK prosecuting authorities

Presenting information orally, as an alternative to written submissions, could in theory reduce the risk that settlement negotiations pose for corporates by limiting the amount of incriminating documentary material generated in settlement negotiations or otherwise provided to the authorities. As a strategy it is obviously conditional on securing the agreement of the prosecuting authority, and is not as frequently encountered in the United Kingdom as in the United States; but the SFO is known to have acceded to requests of this nature on occasion. Notably, this approach was employed in relation to the first and second DPAs entered into in the United Kingdom. However, in the Administrative Court case of *AL v. SFO*,[114] the court, in the context of a criminal trial of individuals following the corporate's[115] entry into a DPA, criticised the use of 'oral proffers' as 'highly artificial' and expressed its surprise that the SFO did not more robustly demand the written notes of interviews made during an internal investigation. The judgment is likely to cause the SFO to be cautious about relying on oral proffers in future investigations and instead to more robustly challenge broad claims to privilege. A senior SFO manager has stated[116] that this decision emphasised the danger for the SFO in not challenging excessively wide claims of privilege. However, given the less restrictive approach taken to legal professional privilege by the Court of Appeal in *ENRC*,

112 Guidance to accompany the Attorney General's Guidelines on Plea Discussions in cases of Serious or Complex Fraud, issued by the Director of Public Prosecutions, the Director of the SFO and the Director of the Revenue and Customs Prosecutions Office, 24 May 2012.

113 Crime and Courts Act 2013 (UK), Schedule 17, para. 5.

114 [2018] EWHC 856.

115 Now known to be Sarclad Limited.

116 Speech given at Herbert Smith Freehills Annual Corporate Crime and Investigations Conference 2018 on 20 June, available at https://www.sfo.gov.uk/2018/06/21/corporate-criminal-liability-ai-and-dpas/.

© Law Business Research 2021

there is likely to be a tension between the authorities' desire to challenge wide claims to privilege and demand written notes of interviews, and the Court of Appeal's decision that written interview notes made during an internal investigation are capable of being covered by litigation privilege. Therefore, although oral proffers may no longer be acceptable, the authorities and co-operating corporates may find themselves in a predicament. The corporate should avoid inadvertent waivers of privilege, and the SFO is also unable to demand written interview notes made while litigation was reasonably in contemplation, and for the dominant purpose of litigation, as interpreted by the Court of Appeal in *ENRC*. In such cases, it is possible that the authorities may stress the importance of a corporate's co-operation in settlement discussions and therefore seek voluntary waivers of privilege over such documents by the corporate.

See Section 23.4

It also raises the prospect that, in multi-agency settlements, there might be a divergence of approach between agencies that are content to receive oral proffers (e.g., the DOJ, which regularly accepts them) and those that are not. Oral summaries of privileged information and material could still be considered by the prosecuting authority as a limited (or indeed full) waiver of privilege, as there is no settled case law in the United Kingdom on this point, which could create a risk of collateral waiver of privilege in other jurisdictions or over other material. If the underlying interviews were not privileged, a prosecutor's notes from the presentation could potentially be disclosed to third parties, without the corporate having an opportunity to confirm whether the impressions recorded are correct.

See Section 23.2.2.1

An indication of the possible approach of courts in the United Kingdom can be gleaned from a ruling in proceedings against Dennis Kerrison and Miltiades Papachristos (employees of Innospec)[117] in which His Honour Judge Goymer considered whether a PowerPoint presentation to the SFO and DOJ that referred to the notes of interviews conducted by the corporate with a prosecution witness amounted to a waiver of legal professional privilege in those interviews. The judge decided that there was not sufficient deployment of the interview notes in the PowerPoint presentation such as would amount to a collateral waiver of legal professional privilege in respect of those notes. It was conceded in argument that the PowerPoint presentation was subject to privilege, and as such there was no detailed discussion of the application of the principles of litigation privilege in this case. This is not always so in the investigations context, following *Three Rivers No. 5*,[118] although as stated above, the Court of Appeal decision in *ENRC* should provide more comfort that interview notes made during an investigation can be covered by litigation privilege if the 'dominant purpose' test is established. The Court of Appeal also considered the ambit of litigation privilege in one of the many cases relating to

117 13 May 2013 unreported.

118 *Three Rivers District Council and Others v. The Governor and Company of the Bank of England* [2003] EWCA Civ 474.

© Law Business Research 2021

the SFO's investigation into the Tchenguiz brothers, stressing the importance of the 'dominant purpose' test.[119]

23.3 Legal considerations

Settlement negotiations should only be undertaken with a thorough understanding of the legal framework that governs the particular form of settlement pursued, and any relevant policies that govern the approach adopted by the relevant prosecuting authority. A number of relevant legal principles will also need to be borne in mind as crucial background context, regardless of the form of settlement pursued.

23.3.1 Legal professional privilege

Prosecuting authorities are increasingly requesting or encouraging corporates to waive privilege as a sign of their co-operation, or even as a precondition to concluding a settlement. The extent to which the prosecuting authority and a corporate may diverge in their interpretations or application of legal professional privilege (LPP) is dealt with in Chapter 36 but the appropriateness of putting pressure on a corporate to waive LPP is far from clear; particularly in the context of a multi-jurisdictional investigation where a number of different legal systems may be in play, all with varying degrees of protection for lawyer–client communications. The collateral damage to the corporate's interests in other jurisdictions if LPP were to be waived could potentially be substantial, and would need to be carefully considered before the corporate agreed to a global settlement involving a waiver on this basis. Attempts to resolve these difficulties by offering limited waiver may work but in practice are certainly not without risk (including, in particular, in relation to collateral waiver risks in: jurisdictions that do not recognise limited waiver; and subsequent related proceedings, as demonstrated by the High Court's decision in *PCP Capital Partners LLP v. Barclays Bank Plc*).

The SFO's guidance on corporate co-operation[120] states that a corporate that does not waive privilege and provide witness accounts will not attain the corresponding factor against prosecution found in the DPA Code, although the corporate will not be penalised by the SFO for electing against waiving privilege. This guidance also states that, if a corporate claims privilege during an investigation, the SFO will expect it to 'provide certification by independent counsel that the material in question is privileged'. How this will work in practice remains to be seen.

119 *Tchenguiz v. Director of the Serious Fraud Office (Non-Party Disclosure)*, also known as *Rawlinson and Hunter Trustees SA v. Akers* [2014] EWCA Civ 136, para. 15.

120 Corporate Co-operation Guidance, issued by the SFO, 6 August 2019. See also the SFO's guidance regarding DPAs in a new chapter of its Operational Handbook, published in October 2020.

© Law Business Research 2021

Admissions 23.3.2

Unlike a plea agreement, the settlement of criminal proceedings by way of a CRO or DPA does not require the corporate to make formal admissions of guilt. However, the effect in practice of agreeing to a CRO or a DPA may be equivalent to an admission. An application for a CRO will be accompanied by a detailed statement of claim,[121] and by agreeing to the CRO the defendant may be taken as confirming its agreement to the contents. Similarly, whereas an admission is not a prerequisite for a DPA, once the DPA is approved, the statement of facts on which it is based becomes admissible in subsequent proceedings in England and Wales (not limited to related criminal proceedings) as if it were the corporate's admission of its contents. In the, *G4S C&J* DPA, Davis J opined that there is no material distinction between a conviction after an early plea of guilty and the admission made as part of the DPA.[122]

Indirect admissions of this kind entail risk for both the corporate and any other persons concerned in the conduct. They could potentially be relied on by third parties in support of civil or criminal proceedings brought against the corporate, both in the United Kingdom and overseas. They are also likely to prejudice the position of any other persons concerned in the conduct, not limited to the corporate's officers. This exposure increases the more extensive the indirect admissions are. In negotiating the first UK DPA, the SFO considered it necessary for the statement of facts to be lengthy (55 pages) to put the judge in a position to approve the agreement on the most complete basis available. The other approved statements of fact published subsequently generally follow a similar approach, although they consistently contain slightly less detail and are shorter. Notably, the GSL's DPA was accompanied by a particularly short statement of facts (17 pages).

A corporate could seek to avoid or at least mitigate some of these adverse consequences by concluding a settlement under which a subsidiary accepts liability and makes any necessary admissions, as in the MW Kellogg Limited CRO in 2011.[123] Note, however, that a corporate will not be able to hide behind a subsidiary that has been set up as a vehicle through which a corrupt payment may be made so that the subsidiary can be abandoned if the corrupt payment comes to light.[124] Alternatively, a corporate could seek to negotiate a settlement under which an individual officer accepts liability instead of the corporate. However, if there is a prospect of a successful prosecution of the corporate entity, this may be unlikely to succeed. As a general matter, risk mitigation strategies of

121 Practice Direction – Civil Recovery Orders, paras. 4.1 to 4.5.

122 *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, paras. 31 and 32.

123 'MW Kellogg Limited to pay £7 million in SFO High Court action', press release dated 16 February 2011, SFO.

124 *XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509, para. 28.

© Law Business Research 2021

this kind are likely to be highly context-specific, and subject to the willingness of the relevant prosecuting authorities to recognise the interests at stake.

23.4 Practical issues arising from the negotiation of UK DPAs

DPAs have to date been made available only for a limited range of corporate economic offences prosecuted by either the CPS or the SFO. Statute governs eligibility for a DPA, its contents and the manner in which it is to be negotiated and approved, with limited discretion left to either the corporate or the prosecuting authority. This departure from the much more flexible US model complicates any predictions as to how frequently DPAs will be relied on in practice in the United Kingdom, but this section will consider practical issues arising from negotiating a DPA in the UK as part of a global settlement.

The legislation requires the judge hearing the application to be satisfied that a DPA is in the interests of justice (as opposed to prosecution of the corporate). The first four agreed DPAs, *Standard Bank plc*, *XYZ Ltd (Sarclad)*, *Rolls-Royce* and *Tesco Stores Limited*, were all heard by Sir Brian Leveson, the former President of the Queen's Bench Division, who (as is clear from the judgments) went to considerable lengths to satisfy himself that the proposed DPAs were in the interests of justice and that the terms were fair, reasonable and proportionate. Notably, in *Rolls-Royce,* he said that the involvement of prosecutors in different countries (in this case, the United States and Brazil) should not preclude a DPA in the United Kingdom, but the extension of criminality to these countries is relevant to the balancing exercise of whether the DPA is in the interests of justice.[125] Following Leveson P's retirement in 2019, Davis J heard the fifth, sixth and eighth DPAs, *Serco Geografix Limited*, *GSL* and *G4S C&J*, whereas Sharp P heard the seventh DPA, *Airbus*. Both Davis J and Sharp P adopted a similar approach to Leveson P. Mrs Justice May heard the ninth DPA, *Airline Services Limited,* and the eleventh and twelfth (under reporting restrictions as at the date of publication) and Lord Justice Edis heard the tenth, AFWEL; and it appears that both again adopted a similar approach to Leveson P.

In the *Standard Bank* decision, Leveson P noted that the first consideration must be the seriousness of the conduct and in this regard emphasised that the potential criminality faced by the bank was the failure to prevent intended bribery committed by senior officers of a sister company. He also noted the SFO's conclusion that there was insufficient evidence to suggest that any of Standard Bank's employees had committed an offence. Nevertheless, in both the *Rolls-Royce* and *Airbus* DPAs, the conduct of the companies was described as some of the 'most serious' breaches of criminal law (*Rolls-Royce*)[126] and 'grave . . . extending into every continent in which Airbus operates' (*Airbus*)[127] but DPAs were ultimately in the interests of justice because of the extent of other factors,

125 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 42.

126 ibid., para. 4.

127 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, paras. 5 and 64.

© Law Business Research 2021

demonstrating that, in certain circumstances, the seriousness of the conduct need not be a bar for a company looking to agree a DPA with the authorities. Leveson P and Sharp P considered in particular the extent of the negative impact that a prosecution of the companies would have had on employees and others innocent of any misconduct such as pensioners or third-party suppliers – factors that were taken into account when balancing the public interest and interests of justice in ultimately approving the DPA. Airbus calculated that the financial impact of debarment would exceed €200 billion, and this could, according to a report that was commissioned by the company, decrease the gross domestic product of each of the US, UK, France, Germany and Spain by over €100 billion.[128] The public interest factors in *Serco Geografix Limited* also outweighed the seriousness of the offence, despite Davis J describing it as 'a substantial fraud' reflecting business practices 'apparently ingrained in the company' and which was compounded by the serious impact the conduct had on the integrity of outsourcing public functions to private companies.[129] In *Serco Geografix Limited* and *G4S C&J*, Davis J expressed reservations about placing weight on the risk of mandatory debarment to support a DPA as this could involve the court making a quasi-political decision.[130] Sharp P in *Airbus* distinguished between scenarios where the risk is of mandatory debarment (considered in *Serco*) as opposed to discretionary debarment (relevant in *Airbus*) coupled with either mandatory or discretionary debarment in other jurisdictions. Sharp P's emphasis was not on the loss of contracts caused by debarment but on the consequential impact this would have on the company, its innocent employees, third parties and the economy.[131]

Leveson P also attached considerable weight to the early report made by Standard Bank to the authorities. He also noted that the bank had made significant enhancements to its compliance policies and procedures since 2011 and that the bank as at November 2015 was effectively a different entity from that which had been involved in the events that were the subject of the DPA. Notably, these two factors were also critical in the other seven DPAs.[132] However, in *Rolls-Royce* there was no self-report; the SFO having been prompted to ask questions of the company by public postings on the internet. Rolls-Royce's co-operation with the SFO was praised by Leveson P, who found that the

128 ibid., paras 85 and 86.

129 *Serco Geografix Limited* [2019] 7 WLUK 45, [2019] Lloyd's Rep FC 518, para. 22.

130 ibid., para. 27; *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, para. 33.

131 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, paras. 84 to 86.

132 *XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509, paras. 15 to 18; *Rolls-Royce*, Crown Court (Southwark), 17 January 2017, paras. 48 to 51, 60 and 63; *Tesco Stores Limited* (Case No. U20170287) [2017] 4 WLUK 558, paras. 51 to 60; and *Serco Geografix Limited* [2019] 7 WLUK 45, [2019] Lloyd's Rep FC 518, paras. 23, 25; *Güralp Systems Limited* (Case No. U20190840) [2019], paras. 5, 27, 30, 49 to 50; *Airbus* (Case No. U20200108) [2020], paras. 68 to 74 and 78 to 80; and *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, paras. 27 to 28 and 40.

© Law Business Research 2021

company could not have done more to expose its own misconduct, limited neither by time, jurisdiction nor area of business. It is this co-operation, in conjunction with extensive ethics and compliance measures and procedures that the company had put in place, and were committed to continuing, that was determinate in the agreement of a DPA, despite the lack of self-reporting.

In *Serco Geografix Limited,* Davis J also placed significant weight on the fact that Serco Geografix Limited was a dormant company, meaning that the obligations imposed on it under the DPA were of limited value, whereas the decision of its parent, Serco Plc, to provide undertakings 'of genuine and substantial effect' allowed the goals of the DPA to be achieved, which he described as an important development in the use of DPAs.[133] The undertaking given by the parent company, G4S, to adopt the compliance measures across the whole group were in G4S C&J's DPA referred to by Davis J as being 'of even greater significance' since the subsidiary, G4S C&J, continued to be in operation in a substantial way.[134]

DPA negotiations are held under strict confidentiality restrictions imposed by the SFO pursuant to the DPA Code of Practice. The Code of Practice requires the corporate entering into DPA negotiations to provide an undertaking in respect of the confidentiality of the fact the DPA negotiations are taking place.

What this means in practice is that third parties with whom the corporate needs to share the fact of the negotiations or any information relating to the DPA negotiations must sign a confidentiality undertaking. Any potential disclosure to the market has to be carefully considered and discussed with the SFO at an early stage (i.e., prior to the relevant obligation arising), and with the judge once an application to the court has been made.[135] Rule 5.8 Criminal Procedure Rules 2015 stipulates that details of a court hearing must appear on the court list at most 48 hours before the court hearing, and the listing must include the names of the parties. This in itself may give rise to press and market speculation on the subject matter of the DPA and the size of the financial penalty. If an announcement is required, an application should be made to the nominated judge.

The legislation does not address anonymity of individuals in the statement of facts. Interestingly, the AFWEL DPA contains a note on its face highlighting that in the case the court considered individual conduct only to assess

133 *Serco Geografix Limited* [2019] 7 WLUK 45, [2019] Lloyd's Rep FC 518, para. 42: 'The nature of modern corporate structures means that it may be problematic to show that a controlling mind of the parent company was involved in the criminality carried out by a subsidiary company even where the benefit of the criminality tended to accrue to the parent company. Yet it will be the parent company which necessarily must engage in any compliance programme and cooperate with law enforcement agencies. The approach taken by Serco Group PLC in this case strengthens the public interest in the approval of this DPA.'

134 *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, para. 43.

135 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 14.

© Law Business Research 2021

the culpability of AFWEL: there was no other reason for the court to consider individuals' involvement in the matter, and the court did not make any findings of facts against any individuals. There are protections afforded in US DPAs and in the course of FCA investigations by the third-party rights provisions, and by the 'Maxwellisation' process in public inquiries. In *Standard Bank plc*, the conclusion reached was that those named on the draft indictment would be named, as would be the bank's senior deal team member, but that the remaining individuals whose conduct was relevant to the factual narrative would remain anonymous. The potential consequences of the naming of individuals following the DPA's publication can be seen in the fact that Ms Shose Sinare, one of the Tanzanian individuals allegedly responsible for the underlying offence in *Standard Bank plc*, has brought a civil claim against Standard Bank in the Tanzanian courts alleging, among other things, that she had a right to see and respond to the allegations in the statement of facts. In both *G4S C&J* and *Airbus*, the anonymity of individuals involved was preserved to avoid any prejudice to the investigation into, and possible prosecution of, individuals.[136]

Tesco Stores Limited, *XYZ Ltd (Sarclad), Serco Geografix Limited*,[137] *GSL and G4S C&J*[138] are the only cases to date where the SFO has pursued charges against individuals following entry into a DPA, although investigations remain ongoing in respect of *Airline Services Limited*, *AFWEL* and the two companies subject to the 11th and 12th DPAs (which remain under reporting restrictions). The DPA judgment in *Tesco Stores Limited* was embargoed for almost two years pending the conclusion of the prosecution of the three former employees, owing to the risk of the details of the DPA undermining or prejudicing those proceedings.[139] The first trial of the three former employees was abandoned after the former UK financial director suffered a heart attack. The former UK managing director and former UK food commercial director were retried and acquitted of all charges, after the trial judge ruled that they had no case to answer. The trial judge's decision was upheld, in emphatic terms, by the Court of Appeal. Subsequently, the former UK financial director, who had been severed from the

136 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, para. 13; *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, para. 45.

137 On 16 December 2019, the SFO announced that it had charged two individuals with fraud and false accounting in relation to its investigations into Serco Geografix Limited. The trial commenced in January 2021 at Southwark Crown Court. However, in April 2021, the trial collapsed following the SFO's failure to disclose evidence to the defendants.

138 On 8 September 2020, the SFO announced that it had charged three former executives of G4S C&J with multiple offences in relation to a multi-year scheme to defraud the Ministry of Justice. The executives were each charged with seven offences of fraud in connection with false representations made to the Ministry of Justice between 2009 and 2012. The original trial date of 6 October 2020 has been postponed until January 2023.

139 As Tesco plc had publicly announced entering into the DPA, and its quantum, pursuant to its regulatory obligations as a publicly listed company, no attempt was made to anonymise its identity.

© Law Business Research 2021

retrial, was acquitted of all charges after the SFO offered no evidence, and the embargo on the DPA was lifted on the same day. Counsel for the three former employees had made representations to Leveson P, both before the DPA was approved and also before it was published, that the statement of facts should be published in a form that did not identify the three former employees, as it would be unfair for the individuals' names and the conduct ascribed to them in the DPA to be publicly available in perpetuity when they had not been found to have committed any offence. On each occasion the request was declined, on the basis that the statement of facts had been ratified by that stage and the legislation does not address anonymity of individuals.

XYZ Ltd (Sarclad) was anonymised on the basis that there were ongoing criminal proceedings arising out of the same facts; to avoid the risk of prejudice in those proceedings, the court ordered that the judgment providing full details of the parties involved only be made public following the conclusion of those proceedings.[140] Sarclad was a small company and was charged with both substantive offences, requiring the application of the identification principle through the involvement of very senior former employees, and for the offence of failing to prevent bribery under the Bribery Act, which may have related to both agents and employees. On 16 July 2019, all three defendants were acquitted of all counts and the judgment providing full details of the facts, the DPA and the statement of facts were published.

See Section 23.1

GSL followed a similar approach to *Tesco Stores Limited* whereby the DPA was agreed on 22 October 2019 but embargoed until the conclusion of the trial of three individuals which took place two months later on 20 December 2019.[141] In the DPA, GSL accepted liability for conspiring to make corrupt payments contrary to section 1 of the Criminal Law Act 1977 and section 1 of the Prevention of Corruption Act 1906 and for failing to prevent bribery by its employees contrary to section 7 of the Bribery Act 2010.[142] As with the *XYZ Ltd (Sarclad)* and *Tesco Stores Limited* DPAs, the individuals were identified in the publicly available DPA judgment and the statement of facts and said to have committed criminal offences, despite having been acquitted of all counts.

The *Tesco Stores Limited, XYZ Ltd (Sarclad) and GSL* DPAs have led to strong calls from a wide range of practitioners and commentators that consideration be given to introducing mechanisms to protect the interests of individuals in the DPA process. A DPA is likely to take less time than a contested trial, so the basis of the DPA will normally be determined before any trial of individuals, which creates a risk that the findings of fact will differ between the two. This risk arises whenever different people are the arbiters of fact, but it is heightened in these circumstances, as the DPA process requires close co-operation between the prosecutors and company to agree on the facts,

140 *XYZ Ltd (Sarclad)* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509, para. 3; *G4S C&J* (Case No. U20201392) [2020] 7 WLUK 303, para. 45.

141 *Güralp Systems Ltd* (Case No U20190840) [2019], paras. 46 to 48.

142 Deferred Prosecution Agreement for *Güralp Systems Limited* (Case No. U20190840) [2019].

© Law Business Research 2021

whereas a trial is a judicially overseen adversarial process in which the jury decides any issues in dispute. Additionally, the company may not have access to the evidence of the natural persons under investigation at the time of a DPA negotiation (e.g., the enforcement agency may have requested the company not to interview the individuals or the individuals may have refused to answer questions at interview, for fear of self-incrimination) and may only come to understand their position if they enter the witness box.

Rolls-Royce did not include the identities of the individuals involved in the criminal conduct for the same reason of avoiding prejudice to potential criminal proceedings.[143] In addition to this, the Court did not name the recipients of corrupt payments or bribes in certain countries on the basis that that this could lead to action or the imposition of penalties which would be regarded in the UK as contravening Article 3 of the European Convention on Human Rights.[144] The same approach was adopted in *Airbus*.[145] The *Rolls-Royce* DPA itself says in terms that it does not provide any protection against prosecution of any present or former officer, director, employee or agent of Rolls-Royce, and further, Rolls-Royce is required to co-operate with the investigation and prosecution of the individuals involved in the relevant conduct.[146] However, the SFO ultimately decided against prosecuting any individuals in the Rolls-Royce investigation.[147]

The negotiation process in *Standard Bank plc* did not move as quickly as originally anticipated. It became apparent that an adversarial stance would not be appropriate in seeking to negotiate an agreement, and over time communications became more focused and more effective. It is also clear from the facts available that *XYZ Ltd (Sarclad)* and *Rolls-Royce* took considerable periods to resolve; so, while the process towards a DPA is likely to be shorter than a contested trial, it will probably still take a considerable period to agree and be approved.

Before the preliminary application is filed at court by the SFO, the corporate is required to provide a declaration regarding the information supplied to the SFO, as well as the declaration of the individual through whom the corporate made its declaration. The declarations are required to be made pursuant to the Criminal Procedure Rules 2015.[148]

To provide comfort to the corporate and the individual it may be necessary to follow a similar process to that used when individuals sign regulatory attestations – including understanding the documentation provided and questioning

143 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, para. 32.

144 ibid.

145 Airbus (Case No. U20200108) [2020] 1 WLUK 435, para. 13.

146 ibid., paras. 71, 72.

147 https://www.sfo.gov.uk/2019/02/22/sfo-closes-glaxosmithkline-investigation-and-investigation-into-rolls-royce-individuals/.

148 Criminal Procedure Rules 2015 No. 1490 (L.18), Rule 11.2(3)(c).

© Law Business Research 2021

those involved in the data collection process. This is something to consider as early as possible in the DPA negotiations.

It is also clearly important to seek to ensure that the scope of any compliance review or monitorship is limited to the matters that are relevant to the circumstances of the case, as these can be intrusive, lengthy and costly exercises. The SFO in *Airbus* did not request the appointment of an external monitor as part of the DPA in light of the extent of Airbus' reform to its compliance procedures and the fact that the French CJIP required ongoing monitoring of Airbus by the French state anti-corruption agency.[149]

In global investigations and settlement discussions it is essential to keep in close contact with other investigating agencies, where necessary providing detailed explanations of the DPA process and the basis on which the statement of facts and DPA terms have been agreed.

23.5 Resolving parallel investigations

In the United Kingdom, historically civil proceedings were generally stayed pending the outcome of any parallel criminal proceedings. This approach was adopted by the High Court in *PCP Capital Partners LLP v. Barclays Bank Plc* who agreed to stay the civil proceedings against the bank pending the resolution of the SFO's criminal proceedings against Barclays and former executives. The civil proceedings were stayed until the outcome of the criminal trial, which ended with the acquittal of the three defendants in February 2020 following a retrial. (The charges against Barclays were dismissed in May 2018[150] and against the former chief executive officer, in April 2019.)[151]

However, courts consider this approach case by case and the emphasis has increasingly moved away from the presumption of a stay. Specifically in the context of contemplated CROs, the current policy (set out in the Attorney General's Guidelines on asset recovery)[152] should prevent civil recovery proceedings from being pursued in parallel with criminal proceedings; although the Bruce Hall example discussed above demonstrates there is no bar against such proceedings being pursued in tandem with criminal proceedings provided the conduct that is the subject of the respective proceedings can be appropriately distinguished.[153]

149 *Airbus* (Case No. U20200108) [2020] 1 WLUK 435, paras. 80 to 81.

150 *R v. Barclays Plc and Barclays Bank Plc* [2018] (Southwark Crown Court) and *The Serious Fraud Office v. Barclays Plc & ANR* [2018] EWHC 3055 (QB).

151 *R v. Varley, Jenkins, Kalaris and Boath* [2019] (Southwark Crown Court) and *R v. Varley, Jenkins, Kalaris and Boath* [2019] EWCA Crim 1074.

152 Guidance for prosecutors and investigators on their asset recovery powers under s.2A Proceeds of Crime Act 2002, 29 November 2012, Attorney General's Office.

153 cf. Thomas LJ in *Innospec*.

© Law Business Research 2021

Other domestic authorities 23.5.1

We have already identified some of the difficulties of negotiating a truly 'global' settlement and their inherent limitations; many of which are equally relevant where there are multiple domestic authorities investigating the same conduct and both civil and criminal proceedings are in contemplation. Corporates seeking to reach a settlement with other domestic authorities are likely to be assisted by agreements and memoranda of understanding (MOU) already in place between the main authorities, including, for example, the MOU between the Competition and Markets Authority and the SFO,[154] and the FCA's Enforcement Guide.[155] The DPA agreed between the SFO and Tesco Stores Limited was coordinated with an agreement with the FCA that Tesco Stores Limited and its parent company, Tesco plc, had committed market abuse.[156] Leveson P did not order Tesco Stores Limited to pay any compensation as part of the DPA as the SFO had said that this would not be a straightforward position; the SFO had not been approached by any investor seeking compensation; and Tesco plc and Tesco Stores Limited had previously agreed with the FCA to pay an estimated £84.4 million under a statutory compensation scheme. The UK criminal courts have historically been reluctant to determine complex issues of compensation and this case demonstrates how DPAs can work in conjunction with regulatory arrangements to compensate victims.

Foreign authorities 23.5.2

The interplay of agencies becomes even more complex where foreign agencies are involved. The participation of UK authorities in global settlements has to date typically been driven by the US authorities, reflecting the relative ease with which US prosecutors can establish corporate criminal liability. However, the more recent example of *Airbus*, which was led from an early stage by the PNF, demonstrates that other investigating authorities may be more willing to take the lead in future global settlements. One potential issue with having multiple agencies involved arises from divergent and sometimes conflicting requests from authorities, typically in connection with communications, disclosure of materials and confidentiality. The aim of any settlement negotiations should be to encourage one authority to take the lead, in accordance with any applicable guidelines or agreements concluded by the relevant authorities for this purpose.

154 Memorandum of understanding between the Competition and Markets Authority and the Serious Fraud Office, 29 April 2014.

155 FCA Handbook, Enforcement Guide, E.G. 12 and E.G. Appendices 2 and 3.

156 'Tesco to pay redress for market abuse', press release, 28 March 2017, FCA.

© Law Business Research 2021

24

Negotiating Global Settlements: The US Perspective

Nicolas Bourtin[1]

24.1 Introduction

Strong incentives exist for corporations – particularly those in highly regulated industries vulnerable to potentially debilitating collateral consequences – to avoid litigating a case brought by the government. Among other considerations, protracted and unpredictable litigation can create risks of (1) financial and reputational harm to the company, (2) weakening relationships with regulators, (3) significant legal expense, and (4) severe legal and regulatory consequences associated with an unfavourable litigation outcome. As a result, when threatened with enforcement action or indictment, corporations often seek to enter into settlement negotiations with investigating authorities. Nevertheless, a corporation entering into such negotiations must carefully weigh the various attendant burdens and collateral consequences of such agreements.

24.2 Strategic considerations

As a preliminary matter, it is important to consider the impact of all interactions with US authorities on the company's ability to reach a settlement on favourable terms. Even early in an investigation, a corporation can develop a co-operative working relationship with authorities through prompt and complete disclosure and assistance with requests and inquiries. While co-operation is not the right strategic approach in all cases – companies may choose to take a more adversarial approach, even early in an investigation – establishing a record of proactive and complete co-operation can have a substantial effect on the final

1 Nicolas Bourtin is a partner at Sullivan & Cromwell LLP. The author acknowledges the contributions of Sullivan & Cromwell associate Steve A Hsieh and former associates Kate Doniger, Stephanie Heglund and Ryan Galisewski to earlier editions of this chapter.

© Law Business Research 2021

terms of any resolution, as US government authorities typically consider the nature and extent of a corporation's co-operation with the investigation in contemplating whether to settle a matter and on what terms. Indeed, both the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC, or the Commission) have explicitly included voluntary disclosure and co-operation in their enforcement policies. As outlined in the DOJ's Justice Manual, in determining whether and to what extent to award a company co-operation credit, the DOJ considers, among other things, 'the timeliness of the co-operation, the diligence, thoroughness and speed of the internal investigation, and the proactive nature of the co-operation'.[2] Similarly, the SEC Enforcement Manual provides that a company's co-operation is evaluated by considering self-policing, self-reporting of misconduct, remediation and co-operation with the investigation.[3] As a result, by conducting an internal investigation and self-reporting potential misconduct to the authorities, a corporation may increase its chances of receiving co-operation credit and, in turn, more favourable settlement terms.[4]

At the close of the government's investigation, when beginning to negotiate the terms of a potential settlement agreement, a corporation must be

2 US Dep't of Justice (DOJ), Justice Manual (JM) § 9-28.700, Principles of Federal Prosecution of Business Organizations, The Value of Cooperation (updated Nov. 2018); see also Justice Manual § 9-47.120, FCPA Corporate Enforcement Policy (updated Nov. 2019). On 20 November 2019, the DOJ announced further revisions to its Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy that, while modest, reflect the DOJ's commitment to providing incentives for companies to self-disclose suspected FCPA violations. The policy revision makes clear that a company's notice to the DOJ of potential criminal conduct can earn it self-reporting credit even if the company does not at the time of the notification understand the full scope of the conduct or the involvement of all relevant employees. In such circumstances, the DOJ will not later penalise the company's self-reporting for failure to include 'all relevant facts'. On 3 July 2020, the DOJ and the Enforcement Division of the SEC released the second edition of 'A Resource Guide to the US Foreign Corrupt Practices Act', which incorporated a number of DOJ policies, including the November 2017 FCPA Corporate Enforcement Policy that set forth incentives for companies to self-disclose, fully co-operate and remediate, including the presumption of a declination in certain circumstances.

3 SEC, Office of Chief Counsel, Enforcement Manual, Framework for Evaluating Cooperation by Companies § 6.1.2 (28 Nov. 2017).

4 Declination in World Acceptance Corp. (5 Aug. 2020), https://www.justice.gov/criminal-fraud/file/1301826/download (declining FCPA prosecution because of, among other reasons, prompt, voluntary self-disclosure; full and proactive co-operation; and full remediation); Declination in Quad/Graphics Inc. (19 Sep. 2019), https://www.justice.gov/criminal-fraud/file/1205341/download (same); Declination in Cognizant Technology Solutions Corporation (13 Feb. 2019), https://www.justice.gov/criminal-fraud/file/1132666/download (same); Non-prosecution Agreement in Akamai Technologies, Inc. (7 Jun. 2016), https://www.sec.gov/news/press/2016/2016-109-npa-akamai.pdf (conditioning non-prosecution agreement (NPA) on 'full, truthful, and continuing cooperation'); Non-prosecution Agreement in Nortek, Inc. (7 Jun. 2016), https://www.sec.gov/news/press/2016/2016-109-npa-nortek.pdf (same).

© Law Business Research 2021

particularly attuned to both the timing and the breadth of such an agreement. Regarding timing, certain stages of litigation can be particularly costly for a corporation; securing settlements early may be advantageous for a corporation. For example, in some cases – particularly where the key facts are known early and there is public pressure on the government to act quickly – a speedy settlement may be struck before a lengthy and expensive investigation is conducted. Such circumstances are rare, however, and the government will normally be reluctant to reach a settlement before a full investigation has been completed.

A more common timing consideration is whether settlement can be achieved before indictment or the filing of a complaint, as such public actions carry the risk of significant legal, financial and reputational consequences. Most negotiated corporate resolutions are reached before charges are filed, as companies are eager to avoid the uncertain public and shareholder reaction to a contested litigation. Economic studies show that a company's share price generally decreases more dramatically as a result of the announcement of a government investigation if there is no concurrent resolution.[5] The extent of share price declines can, among other effects, have great significance in follow-on civil litigation.

In terms of the breadth of a potential settlement agreement, a corporation must consider the scope of the conduct being investigated and the scope of the potential release from liability. At the conclusion of the government's investigation, to the extent that it opts to pursue charges related to certain alleged misconduct, it can be advantageous for those charges to be reflected in a single settlement agreement or in distinct agreements announced simultaneously, so as to mitigate the risk of legal, financial and reputational harm associated with multiple days of negative press, carry-over investigations and future litigation.

5 See Declaration of Stephen Choi, Ph.D., *In re Goldman Sachs Grp., Inc. Sec. Litig.*, No. 1:10-cv-03461-PAC, 2015 WL 5613150 (S.D.N.Y. 6 Apr. 2015), ECF No. 145 (finding that the average impact of an investigation announcement was -3.8 per cent when there was no concurrent resolution, compared to 0.22 per cent when there was a concurrent resolution). Compare Christian Flore et al., Settlement Agreement Types of Federal Corporate Prosecution in the US and Their Impact on Shareholder Wealth, 76 Journal of Business Research 145, 157 (2017) (analysing corporate settlements – 100 plea agreements, 64 deferred prosecution agreements (DPAs) and 63 NPAs between January 2001 and December 2014 – and their effect on shareholder wealth and concluding 'significant and positive shareholder wealth effects to the announcement of settlement, indicating that investors generally view settlements as positive information') with Gus De Franco et al., The Effect of Deferred Prosecution Agreements on Firm Performance, https://accounting.wharton.upenn.edu/wp-content/uploads/2019/10/De-Franco-Small-and-Wahid-2019-WP.pdf (finding that 'firms subject to DPAs experience significantly lower buy-and-hold returns in the one- to three-year period following the DPA compared with prosecuted firms' and that 'DPA firms experience negative real consequences following the initiation of a DPA, relative to prosecuted firms, as measured by decreases in both sales and the number of employees'; concluding that findings are 'inconsistent with the idea that DPAs reduce the collateral damage to stakeholders who are not responsible for the crimes committed by the organization (i.e., innocent parties)').

© Law Business Research 2021

In the event that the government determines not to pursue charges against the company or its employees,[6] it can be advantageous to diplomatically encourage a 'declination' – a formal notice that the government has declined to pursue the case further[7] – to provide the company valuable closure.

Owing to the government's focus on the prosecution of individuals, however, it is unlikely that the government will release from liability company employees who engaged in potential wrongdoing as part of a settlement with a company.[8]

---

6 The Justice Manual lists 11 factors that prosecutors should weigh in determining whether to charge a corporation: (1) the nature and seriousness of the offence; (2) the pervasiveness of wrongdoing within the corporation; (3) the corporation's history of similar misconduct; (4) the corporation's willingness to co-operate including as to potential wrongdoing by its agents; (5) the adequacy and effectiveness of the corporation's pre-existing compliance programme; (6) the corporation's timely and voluntary disclosure of wrongdoing; (7) the corporation's remedial actions; (8) collateral consequences; (9) the adequacy of other remedies; (10) the adequacy of the prosecution of individuals responsible for the corporation's malfeasance; and (11) the interest of any victims. JM § 9-28.300, Principles of Federal Prosecution of Business Organizations, Factors to Be Considered (updated Jul. 2020). The SEC considers its own factors in determining whether to close an investigation, including: (1) the seriousness of the conduct and potential violations; (2) the staff resources available to pursue the investigation; (3) the sufficiency and strength of the evidence; (4) the extent of potential investor harm if an action is not commenced; and (5) the age of the conduct underlying the potential violations. SEC, Office of Chief Counsel, Enforcement Manual § 2.6.1, Policies and Procedures.

7 Precise practices may differ. For example, the DOJ may issue a declination letter reporting that it has closed its investigation or declined to prosecute. See Department of Justice, Fraud Section, Declinations, https://www.justice.gov/criminal-fraud/corporate-enforcement-policy/declinations (last updated 6 Aug. 2020). The policy of the SEC is to send 'termination letters' to 'notify individuals and entities at the earliest opportunity when the staff has determined not to recommend an enforcement action against them to the Commission'. SEC, Office of Chief Counsel, Enforcement Manual § 2.6.2, Termination Notices. These SEC termination letters provide somewhat less assurance than a formal declination, because '[a]ll that such a communication means is that the staff has completed its investigation and that at that time no enforcement action has been recommended to the Commission.' Id.

8 One exception may be found in settlements with the DOJ's Antitrust Division. Historically, antitrust settlements regularly contained non-prosecution provisions that protected a company's employees from criminal liability related to the antitrust activity at issue. Antitrust settlements may 'carve out' certain individuals from this protection based on their level of culpability. See Scott D Hammond, Dep. Ass't Att'y Gen. for Criminal Enforcement, Antitrust Division, Measuring the Value of Second-In Cooperation in Corporate Plea Negotiations, Presented at the ABA Antitrust Section Spring Meeting (29 Mar. 2006), available at https://www.justice.gov/atr/speech/measuring-value-second-cooperation-corporate-plea-negotiations ('Most [antitrust] corporate plea agreements provide a non-prosecution agreement for company employees who cooperate fully in the investigation.'). In July 2019, the Antitrust Division announced a new policy allowing the use of DPAs to resolve criminal antitrust investigations. Makan Delrahim, former Ass't Att'y Gen., Remarks at the New York University School of Law Program on Corporate Compliance and Enforcement (11 Jul. 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers

© Law Business Research 2021

The DOJ formalised its increased focus on the prosecution of individuals with the publication of a 2015 policy memorandum signed by then-Deputy Attorney General Sally Quillian Yates regarding individual accountability for corporate wrongdoing.[9] The 'Yates Memorandum' memorialised certain government sentiments demonstrating an inclination toward the prosecution of individuals in corporate fraud cases,[10] and specified that 'absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation'.[11] Under the Trump administration in 2017, the DOJ revised the Yates Memorandum's guidance to restore some discretion to civil prosecutors, who are now empowered to 'negotiate civil releases for individuals who do not warrant additional investigation in corporate civil settlement agreements'.[12] The revised guidance also stated that a corporation will be

-remarks-new-york-university-school-l-0. In January 2021, a ready-mix concrete company entered into a DPA for fixing prices and rigging bids in violation of antitrust laws. DOJ, Press Release, 'Ready-Mix Concrete Company Admits to Fixing Prices and Rigging Bids in Violation of Antitrust Laws' (4 Jan. 2021), https://www.justice.gov/opa/pr/ready-mix-concrete-company-admits-fixing-prices-and-rigging-bids-violation-antitrust-laws. The DPA was entered into after the indictment of two individuals 'primarily responsible' for the charged conspiracy. *In re Argos USA LLC* (4 Jan. 2021), https://www.justice.gov/opa/press-release/file/1350481/download.

9 See Sally Quillian Yates, Memorandum from the US Dep't of Justice on Individual Accountability for Corporate Wrongdoing (9 Sep. 2015), https://www.justice.gov/dag/file/769036/download (Yates Memorandum).

10 See, e.g., Marshall Miller, Principal Dep. Ass't Att'y Gen. for the Criminal Division, Remarks at the Global Investigations Review Conference (17 Sep. 2014), https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller (explaining that 'when [corporations] come in to discuss the results of an internal investigation to the Criminal Division . . . expect that a primary focus will be on what evidence you uncovered as to culpable individuals, what steps you took to see if individual culpability crept up the corporate ladder, how tireless your efforts were to find the people responsible'); Sung-Hee Suh, Dep. Ass't Att'y Gen., Remarks at the PLI's 14th Annual Institute on Securities Regulation in Europe: Implications for U.S. Law on EU Practice (20 Jan. 2015), https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-sung-hee-suh-speaks-pli-s-14th-annual-institute-securities (explaining that 'corporations do not act criminally, but for the actions of individuals . . . the Criminal Division intends to prosecute those individuals, whether they are sitting on a sales desk or in a corporate suite'); Leslie Caldwell, Ass't Att'y Gen. for the Criminal Division, Remarks at New York University Law School's Program on Corporate Compliance and Enforcement (17 Apr. 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-new-york-university-law (explaining that '[t]rue cooperation . . . requires identifying the individuals actually responsible for the misconduct – be they executives or others – and the provision of all available facts relating to that misconduct').

11 Yates Memorandum at 2.

12 Rod J Rosenstein, Dep. Att'y Gen., Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 Nov. 2018),

© Law Business Research 2021

eligible for co-operation credit if it operates in good faith to identify individuals who were 'substantially' involved in or responsible for the potential misconduct, a move away from the Yates Memorandum's more stringent requirement that 'the company must identify all individuals responsible for the misconduct at issue, regardless of their position, status, or seniority'.[13] The Biden administration returned to the Yates Memorandum's focus on individual prosecutions, stating that 'it is unambiguously [the DOJ's] first priority in corporate criminal matters to prosecute the individuals who commit and profit from corporate malfeasance'.[14] The DOJ thus 'restore[d] prior guidance making clear that to be eligible for any cooperation credit, companies must provide the department with all non-privileged information about individuals involved in or responsible for the misconduct at issue. . . . [A] company must identify all individuals involved in the misconduct, regardless of their position, status or seniority'.[15]

Similarly, in the securities enforcement context, the SEC has expressed a focus on charging individuals responsible for wrongdoing.[16] In particular, Mary Jo White, former Chair of the SEC, highlighted that one approach to charging individuals is to use Section 20(b) of the Exchange Act[17] to target those who have 'engaged in unlawful activity but attempted to insulate themselves from

---

https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0. When announcing these changes, Dep. Att'y Gen. Rod Rosenstein emphasised that this policy shift was in 'response to concerns raised about the inefficiencies of requiring companies to identify every employee involved regardless of relative culpability' and was 'consistent with our commitment to hold individuals accountable in every appropriate case.' Id.

13 Yates Memorandum at 3.

14 Lisa O Monaco, Dep. Att'y Gen., Keynote Address at ABA's 36th National Institute on White Collar Crime (28 Oct. 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

15 Id.

16 Joshua Gallu and David Michaels, 'SEC to Shift Enforcement Focus to Individuals, White Says', *Bloomberg News* (26 Sep. 2013), www.bloomberg.com/news/articles/2013-09-26/sec-to-shift-enforcement-focus-to-individuals-white-says-1-; Mary Jo White, SEC Chair, Speech at the New York City Bar Association's Third Annual White Collar Crime Institute: Three Key Pressure Points in the Current Enforcement Environment (19 May 2014), https://www.sec.gov/news/speech/2014-spch051914mjw.html (noting that an 'internal, back-of-the[-]envelope, analysis the staff did recently indicates that since the beginning of the 2011 fiscal year, we charged individuals in 83% of our actions . . . , [a]nd we look for ways to innovate in order to further strengthen our ability to charge individuals').

17 § 20(b) Securities Act of 1933 allows the Commission to bring enforcement actions against 'any person' who does 'any act or thing which it would be unlawful for such person to do under the provisions of this chapter or any rule or regulation thereunder through or by means of any other person'. See 15 U.S.C. § 78t(b) (2011).

© Law Business Research 2021

liability by avoiding direct communication with the defrauded investors'.[18] The Commissioner of the SEC has continued to focus on individual accountability.[19]

24.3 Legal considerations

24.3.1 Privilege considerations

At times during the investigative process, legal considerations may be in tension with strategic ones – a corporation should be cognisant of the potential for such tensions to navigate toward an agreeable settlement without unnecessarily waiving any valuable rights. In particular, a company may need to weigh the value of additional co-operation credit for disclosing relevant privileged documents to the government against the value of protecting privileged documents from future discovery in follow-on civil litigation.

Under current DOJ policy, for example, 'cooperation credit is not predicated upon the waiver of attorney–client privilege or work-product protection', but co-operation still requires the timely disclosure of 'relevant facts',[20] which may require disclosure of some privileged materials, such as memoranda of witness interviews prepared during an internal investigation.[21] However, disclosure to the government of documents prepared during the course of an investigation may waive any relevant protections during follow-on civil litigation.[22] In such instances, a company may consider entering into a limited waiver agreement with the government as a middle ground, but it must keep in mind that courts

18 Id.

19 Caroline A Crenshaw, SEC Commissioner, Speech: Moving Forward Together – Enforcement for Everyone (9 Mar. 2021), https://www.sec.gov/news/speech/crenshaw-moving-forward-together ('Meaningful cooperation requires a commitment to proactively identifying and remediating wrongdoing, as well as holding accountable those individuals responsible for misconduct.').

20 Justice Manual § 9-28.720, Principles of Federal Prosecution of Business Organizations, Cooperation: Disclosing the Relevant Facts (rev. Nov. 2017).

21 Id.

22 For example, the Second Circuit Court of Appeals held that voluntary submission of a legal memorandum to the SEC during its investigation waived protections of the work-product doctrine in a subsequent civil class action suit. *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 232 (2d Cir. 1993). But the court declined 'to adopt a per se rule that all voluntary disclosures to the government waive work product protection.' Id. at 236. Similarly, a court in the Southern District of New York held that briefs, written memos, white papers and presentations shown to the Commodity Futures Trading Commission (CFTC) were discoverable in a subsequent civil action. See *Alaska Electrical Pension Fund v. Bank of America Corp.*, 2017 WL 280816, at *2, 3 (S.D.N.Y. 20 Jan. 2017). The court's decision, however, noted the lack of confidentiality agreements between the government and the defendants, and the court did not claim to apply a categorical rule about confidentiality agreements and waiver of work-product privilege. See id. at *2. ('[T]he Court need not decide categorically whether confidentiality agreements can ever protect work product that is shared voluntarily with a government agency because, at most, they are just one of several factors to be considered, and they are not enough to carry the day here.' (internal quotation marks and citations omitted)).

© Law Business Research 2021

may be sceptical of a limited waiver agreement, even when paired with a confidentiality agreement.[23]

As part of its investigative process, the government may also engage the company in discussions as to whether charges are warranted. Government authorities may convey this information to the company orally, through reverse

23 Most federal courts of appeal have declined to allow a selective disclosure to regulators during an investigation of documents protected by the attorney–client privilege or work-product doctrine without a resultant waiver of the privilege or protection with respect to third-party civil litigants. See *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127–28 (9th Cir. 2012) (US Attorney investigation); *In re Qwest Commc'ns Int'l, Inc.*, 450 F.3d 1179 (10th Cir. 2006) (SEC and DOJ investigations); *Gruss v. Zwirn*, 2013 WL 3481350, at *5–8 (S.D.N.Y. 10 Jul. 2013) (reviewing 'the origin and current viability of the "selective waiver" doctrine' and reversing the findings of a magistrate judge that a confidentiality agreement with the SEC prevented waiver). See also SEC, Office of Chief Counsel, Enforcement Manual § 4.3.1, Confidentiality Agreements (28 Nov. 2017) ('While obtaining materials that are otherwise potentially subject to privilege or the protections of the attorney work-product doctrine can be of substantial assistance in conducting an investigation, the staff should exercise judgment when deciding whether to enter into a confidentiality agreement with a company under investigation. Considerations include [that] . . . [s]ome courts have held that companies that produce otherwise privileged materials to the SEC or the US Department of Justice, even pursuant to a confidentiality agreement, waived privilege in doing so.'). But see *In re Steinhardt Partners, L.P.*, 9 F.3d. 230, 236 (2d Cir. 1993) ('[W]e decline to adopt a *per se* rule that all voluntary disclosures to the government waive work product protection. . . . Establishing a rigid rule would fail to anticipate . . . situations in which the SEC and the disclosing party have entered into an explicit agreement that the SEC will maintain the confidentiality of the disclosed materials.'); see also *In re Natural Gas Commodity Litigation*, 2005 WL 1457666, at *8 (S.D.N.Y. 21 Jun. 2005) (discussing how an explicit confidentiality agreement combined with a non-waiver agreement went a 'long way' toward establishing non-waiver).

© Law Business Research 2021

proffers,[24] or in writing, through a document such as the SEC's Wells notice.[25] Upon receipt of such information, the company then generally may respond with its arguments as to why the government should not bring an enforcement action. While providing a response is usually advisable and carries the prospect of success, in certain circumstances, a corporation may determine that it is not in the company's best interest. Among other considerations, a Wells submission is not privileged or confidential, and therefore can be used later against the corporation in civil litigation or made publicly available.[26] In fact, the SEC Enforcement Manual provides that the SEC staff may reject any Wells submission that purports to be settlement-related material.[27] In the alternative, the corporation may opt to initiate a meeting with the authorities to discuss the proposed charges to prevent the creation of discoverable material and foster a dialogue between the company and the government.

During settlement negotiations, a corporation must also be careful in sharing drafts of settlement documents because materials shared with the government may become discoverable in civil litigation. Although documents

24 See Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute: The SEC's Cooperation Program: Reflections on Five Years of Experience (13 Mar. 2015), https://www.sec.gov/news/speech/sec-cooperation-program.html. ('One thing we are doing more of is using reverse proffers at key points in our investigations. When appropriate, we will invite counsel in for a meeting in which we share key documents and expected testimony that will implicate the defendant. This is another practice that is well established among criminal prosecutors and FBI agents but historically has been used less frequently at the SEC. Sometimes we might do a reverse proffer at a more advanced stage of an investigation in order to attempt to bring the investigation swiftly to a close on settlement terms that we deem favourable and appropriate. But we also might do it much earlier in an investigation, in order to demonstrate to a witness why cooperation is worthwhile.'); Mary Jo White, SEC Chair, Speech at New York University School of Law Program on Corporate Compliance and Enforcement (18 Nov. 2016), https://www.sec.gov/news/speech/chair-white-speech-new-york-university-111816.html ('When appropriate, we share with defense counsel significant documents and expected testimony, as well as any analyses we have done. We often do reverse proffers at an advanced stage of an investigation in order to attempt to bring the investigation swiftly to a close on strong settlement terms. But we also sometimes do them much earlier in order to demonstrate the benefits of cooperating with our ongoing investigation.').

25 A Wells notice is a letter that a securities or commodities regulator, such as the SEC, CFTC or the Financial Industry Regulatory Authority, sends to a corporation or individual when it intends to bring a civil action against them.

26 Indeed, the SEC Enforcement Manual indicates that advocacy materials presented to the SEC may be discoverable and admissible in evidence, notwithstanding the protections of Federal Rule of Evidence 408. See SEC, Office of Chief Counsel, Enforcement Manual § 3.2.3.2, White Papers and Other Materials (excluding Wells submissions) (28 Nov. 2017). See also *In re Initial Pub. Offering Sec. Litig.*, 2004 WL 60290, at *2 (S.D.N.Y. 12 Jan. 2004) ('Wells submissions are not – or at least, not intrinsically – settlement materials.').

27 See SEC, Office of Chief Counsel, Enforcement Manual, The Wells Process § 2.4 (28 Nov. 2017).

© Law Business Research 2021

related to settlement negotiations are generally protected under Federal Rule of Evidence 408,[28] the documents may nonetheless ultimately be deemed discoverable,[29] or even admissible as evidence.[30]

Limitations and tolling agreements 24.3.2

In the course of a government investigation, statutes of limitations will often come into play.[31] At the outset of an investigation, particularly if the investigation commences toward the end of a particular statutory period, the government may ask the company to sign a tolling agreement, an agreement to waive a right to claim that litigation should be dismissed owing to the expiry of a statute of limitations for a particular period.[32] It may be in the best interest of the company to sign it, as a form of co-operation and to avoid a precipitous filing of charges by the government. If a tolling agreement has not been signed at an earlier stage in the investigation, the government may ask a corporation

28 See Fed. R. Evid. 408 advisory committee's note ('[S]tatements made during compromise negotiations of other disputed claims are not admissible in subsequent criminal litigation, when offered to prove liability for, invalidity of, or amount of those claims.').

29 For example, courts in the Southern District of New York consistently hold that 'Rule 408 does not apply to discovery': e.g., *Morgan Art Found. Ltd. v. McKenzie*, 2020 WL 3578251, at *5 (S.D.N.Y. 1 Jul. 2020); *Republic of Turkey v. Christie's, Inc.*, 326 F.R.D. 394, 399 (S.D.N.Y. 2018); *Small v. Nobel Biocare USA, LLC*, 808 F. Supp. 2d 584, 586 (S.D.N.Y. 2011); accord *Conopco, Inc. v. Wein*, 2007 WL 1040676, at *5 (S.D.N.Y. 4 Apr. 2007); *ABF Capital Mgmt. v. Askin Capital*, 2000 WL 191698, at *1 (S.D.N.Y. 10 Feb. 2000). Rather, courts apply the discovery standard of Federal Rule of Civil Procedure 26(b)(1) to determine the discoverability of settlement negotiations: e.g., *Morgan Art Found.*, 2020 WL 3578251, at *5; *Republic of Turkey*, 326 F.R.D. at 399; *Small*, 808 F. Supp. 2d at 586–87; *ABF Capital Mgmt.*, 2000 WL 191698, at *2.

30 For example, *In re Gen. Motors LLC Ignition Switch Litig.*, 2016 WL 4410008, at *5 (S.D.N.Y. 18 Aug. 2016) (deferring a ruling on the admissibility of evidence concerning 'a voluntary settlement program' but suggesting the use of 'protective measures' such as limiting instructions to the jury and bifurcation of the punitive damages phase of trial); *In re Gen. Motors LLC Ignition Switch Litig.*, 2015 WL 7769524, at *2 (S.D.N.Y. 30 Nov. 2015) (admitting consent decree as evidence 'not . . . to prove that New GM violated the Safety Act . . . but for other purposes that are plainly relevant'); *In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on April 20, 2010*, 2012 WL 413860, at *3 (E.D. La. 9 Feb. 2012) (granting a motion *in limine* to prevent jury from receiving evidence about a DPA that resolved allegations about an earlier oil refinery accident in Texas but deeming DPA potentially relevant for future proceedings, such as punitive damages).

31 Unless otherwise provided by statute, an enforcement action by a federal regulator that seeks a civil fine or penalty is generally subject to the standard five-year limitations period for proceedings. 28 U.S.C. § 2462. 'Securities fraud offenses', however, are subject to six-year limitations periods. 18 U.S.C. § 3301.

32 See SEC, Office of Chief Counsel, Enforcement Manual § 3.1.2, Statutes of Limitations and Tolling Agreements (28 Nov. 2017); DOJ and SEC, A Resource Guide to the US Foreign Corrupt Practices Act at 35 (8 Jul. 2020), https://www.justice.gov/criminal-fraud/file/1292051/download ('[C]ompanies or individuals cooperating with DOJ may enter into a tolling agreement that voluntarily extends the limitations period.').

© Law Business Research 2021

to sign one during the settlement negotiation process, especially if a potential limitations period is about to close. In this context, tolling agreements serve to relieve the government of the pressure of taking formal action before the relevant limitations period runs, and allow for time for additional sharing of information in the hope of facilitating a settlement agreement.[33] A tolling agreement signed by the corporation will not toll the statute of limitations against individuals. Rather, to toll the time to bring charges against an individual, the government will have to secure a separate tolling agreement with that person.[34]

24.4 Forms of resolution

24.4.1 Prosecutorial settlements: DPAs, NPAs and guilty pleas

Most corporate criminal investigations initiated by US prosecutors were resolved by deferred prosecution agreements (DPAs) and non-prosecution

33 See SEC, Office of Chief Counsel, Enforcement Manual § 3.1.2, Statutes of Limitations and Tolling Agreements (28 Nov. 2017) ('If the assigned staff investigating potential violations of the federal securities laws believes that any of the relevant conduct arguably may be outside the five-year limitation period before the SEC would be able to file or institute an enforcement action, the staff may ask the potential defendant or respondent to sign a "tolling agreement." Such requests are occasionally made in the course of settlement negotiations to allow time for sharing of information in furtherance of reaching a settlement.'); Justice Manual § 9-28.210, Focus on Individual Wrongdoers (updated Nov. 2018) ('Every effort should be made to resolve a corporate matter within the statutorily allotted time, and tolling agreements should be the rare exception.').

34 See the Yates Memorandum at 6 ('[W]here it is anticipated that a tolling agreement is . . . unavoidable and necessary, all efforts should be made either to resolve the matter against culpable individuals before the limitations period expires or to preserve the ability to charge individuals by tolling the limitations period by agreement or court order.'); Justice Manual § 4-3.100 (updated Nov. 2018) (same).

© Law Business Research 2021

agreements (NPAs).[35] DPAs and NPAs are generally thought of as a middle ground between declining prosecution and obtaining a conviction.[36]

In an NPA, no criminal charges are filed against the company. As a result, an NPA need not be made public unless prosecutors seek to publicise the results of the investigation or the company is itself required to disclose the agreement. A DPA differs in that the government brings criminal charges against the company, which it agrees to dismiss at the end of a specified period if the company complies with the DPA's terms. Because a DPA is filed with the court, it becomes a public document. Consequently, unlike an NPA, over which the government has full discretion to adopt terms and conditions, a DPA may be subject to some level of judicial review. Because a DPA involves the filing of an information or indictment, the Speedy Trial Act requires trial to start within

35 Although there is no standard form or precedent for these agreements, most prosecutorial settlement agreements include some or all of the following provisions: (1) a statement of facts describing illegal acts or an admission of wrongdoing, or both; (2) an agreement that the company, its employees and its agents will not publicly contradict the statement of facts; (3) co-operation with the government for the duration of the agreement, including the provision of documents and efforts to secure employee testimony; (4) some form of remedial action, including terminating or disciplining culpable employees, implementing revised internal controls and procedures, or, in some cases, appointing an independent compliance monitor; (5) fines and penalties; (6) obligations to report future violations of law; and (7) an acknowledgement that the government has the sole discretion to determine whether the agreement has been breached. For both an NPA and a DPA, because the company has generally admitted to the conduct at issue, if a company is indicted upon breach of the agreement, conviction is almost certain. For examples of DPAs and NPAs, see *In re Goldman Sachs Group Inc.* (22 Oct. 2020), https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion (DPA, FCPA); *In re JPMorgan Chase & Co.* (29 Sep. 2020), https://www.justice.gov/opa/pr/jpmorgan-chase-co-agrees-pay-920-million-connection-schemes-defraud-precious-metals-and-us (DPA, spoofing); *In re Bank Hapoalim B.M.* (30 Apr. 2020), https://www.justice.gov/opa/press-release/file/1275081/download (DPA, money laundering); *Bank Hapoalim B.M.* (30 Apr. 2020), https://www.justice.gov/opa/press-release/file/1272446/download (NPA, tax); *In re Wells Fargo* (21 Feb. 2020), https://www.justice.gov/opa/press-release/file/1251346/download (DPA, criminal and civil sales practices); *UniCredit Bank Austria AG* (15 Apr. 2019), https://www.justice.gov/opa/press-release/file/1154516/download (NPA, IEEPA); *In re Standard Chartered Bank* (9 Apr. 2019), https://www.justice.gov/opa/press-release/file/1152801/download (DPA, IEEPA).

36 See Justice Manual § 9-28.1100, Principles of Federal Prosecution of Business Organizations, Collateral Consequences (updated Jul. 2020) ('[W]here the collateral consequences of a corporate conviction for innocent third parties would be significant, it may be appropriate to consider a non-prosecution or deferred prosecution agreement with conditions designated, among other things, to promote compliance with applicable law and to prevent recidivism. Such agreements are a third option, besides a criminal indictment, on the one hand, and a declination, on the other.').

© Law Business Research 2021

70 days.[37] However, the Speedy Trial Act allows this 70-day period to be tolled with the 'approval of the court, for the purpose of allowing the defendant to demonstrate his good conduct'.[38] Although this provision suggests that courts have a role in overseeing DPAs, judges have historically been relatively deferential to the government in approving them.

Two decisions from the US Courts of Appeals for the District of Columbia and Second Circuit confirm that the long-standing practice of limited judicial oversight over consensual enforcement settlements is the favoured approach. In each case, the district court refused to approve a settlement that the court deemed too lenient, and was reversed by the Court of Appeals on the grounds that the trial court's discretion in such circumstances is quite limited. In April 2016, in *United States v. Fokker Services BV*,[39] the DC Circuit Court of Appeals issued a writ of *mandamus* and vacated a decision by District Judge Richard Leon that rejected as too lenient a proposed DPA between the DOJ and Fokker Services. The Court of Appeals reasoned that 'the court's withholding of approval would amount to a substantial and unwarranted intrusion on the Executive Branch's fundamental prerogatives'.[40] Similarly, in June 2014, the Second Circuit issued a decision in *SEC v. Citigroup Global Markets*,[41] calling into question the appropriateness of judicial scrutiny of consensual settlements with the SEC. In a decision that reversed a notable opinion written by District Judge Jed Rakoff criticising an SEC settlement with Citigroup as insufficient, the Second Circuit made clear that courts must afford the SEC's policy judgements 'significant deference', including whether, when and how to resolve enforcement proceedings.[42] Under *Citigroup*, a district court's review of a settlement agreement is narrow and limited. Subsequent cases have added glosses to the *Citigroup* holding, with some district courts exerting discretion over certain aspects of settlement agreements,[43] including the selection of an independent monitor.[44] Notably, the Second Circuit, in *United States v. HSBC Bank*,[45] overturned a district court's

37 See 18 U.S.C. § 3161(c)(1); see also Justice Manual: Criminal Resource Manual § 628, Speedy Trial Act of 1974 (updated 22 Jan. 2020).

38 18 U.S.C. § 3161(h)(2).

39 818 F.3d 733, 747 (D.C. Cir. 2016), vacating 79 F. Supp. 3d 160 (D.D.C. 2015).

40 Id. at 744.

41 752 F.3d 285 (2d Cir. 2014).

42 Id. at 296–97.

43 See, e.g., *US Securities and Exchange Commission v. Aronson*, 665 F. App'x 78, 80 (2d Cir. 2016) (holding that the district court did not abuse its discretion in ordering briefing on an issue before a related criminal case was completed, even though the consent decree provided that the parties would propose a briefing schedule after completion of the criminal case).

44 See *US Commodity Futures Trading Commission v. Deutsche Bank AG*, 2016 WL 6135664, at *1–3 (S.D.N.Y. 20 Oct. 2016) (holding that it was proper for the court to select an independent monitor, when the parties' proposed monitors were inadequate).

45 863 F.3d 125 (2d Cir. 2017).

© Law Business Research 2021

decision to unseal a monitor's report and found that the district court erred in invoking its supervisory authority over a DPA.

Despite the reversals, the district courts' criticisms are broadly consistent with those expressed in recent years by a number of federal judges who have hesitated before ultimately approving DPAs and other similar government settlements. In those other instances, the courts' criticisms commonly have included assertions that those settlements lacked (1) a large enough penalty amount[46] (relatedly, there is concern that companies will begin to view monetary penalties merely as 'a cost of doing business'),[47] (2) admissions of wrongdoing by the company,[48] (3) charges against the individuals who were responsible for the offence,[49] (4) sufficient factual detail for the judge to evaluate the agreement,[50]

46 See *US v. Saena Tech Corp.*, 140 F. Supp. 3d 11, 31 (D.D.C. 2015) ('An agreement that contained neither punitive measures (such as fines) nor requirements designed to deter future criminality (such as compliance programs and independent monitors) could not be said to be designed to secure a defendant's reformation and should be rejected. Even an agreement that contained some of these elements could be ineffective if the obligations were found to be so vague or minimal as to render them a sham.'); Order Approving Deferred Prosecution Agreement at 2, *United States v. Transp. Logistics Int'l, Inc.*, No. 8:18-cr-00011-TDC, ECF No. 10 (D. Md. 2 Apr. 2018) (commenting that the DPA required 'a criminal penalty that is less than 10 percent of the amount contemplated by the Sentencing Guidelines' and thus risks providing 'insufficient deterrence to companies').

47 See, e.g., Brett Wolf, 'U.S. Warns Banks It May Revoke Some Money-Laundering Settlements', Reuters (15 Mar. 2015), http://www.reuters.com/article/us-banks-moneylaundering-idUSKBN0MC1ZE20150316 (quoting Assistant Attorney General Caldwell as saying 'We don't want DPAs and NPAs to be perceived as a cost of doing business'); Peter J Henning, 'Guilty Pleas and Heavy Fines Seem to Be Cost of Business for Wall St.', *The New York Times* (20 May 2015), https://www.nytimes.com/2015/05/21/business/dealbook/guilty-pleas-and-heavy-fines-seem-to-be-cost-of-business-for-wall-st.html?_r=0 ('Banks appear willing to plead guilty as long as the collateral costs are not too heavy. Thus, the potency of a criminal conviction as a deterrent seems to have been dissipated, perhaps to the point that it is just another business expense.').

48 See, e.g., *S.E.C. v. CR Intrinsic Investors, LLC*, 939 F. Supp. 2d 431, 436–39 (S.D.N.Y. 2013) (discussing concerns about allowing 'neither admit nor deny' provisions in a consent judgment).

49 See *Saena Tech Corp.*, 140 F. Supp 3d at 35–36 (discussing potential concerns with a DPA that effectively immunised an individual).

50 Cf. *US Securities and Exchange Commission v. Mulvaney*, 2012 WL 12930425, at *1 (E.D. Wis. 20 Nov. 2012) (granting consent decree only after ordering further briefing on its factual basis).

© Law Business Research 2021

(5) sufficient remedial obligations for the company[51] and (6) sufficient reporting to the court about the company's compliance with the agreement.[52]

The ability for a company to receive multiple NPAs or DPAs has drawn criticism and the practice may be disfavoured under the Biden administration. In October 2021, the DOJ questioned whether a 'recidivist' company with prior NPAs or DPAs should qualify for another NPA or DPA.[53] Moreover, the DOJ instructed prosecutors that 'all prior misconduct needs to be evaluated when it comes to decisions about the proper resolution with a company, whether or not that misconduct is similar to the conduct at issue in a particular investigation'.[54] This includes those within and outside the DOJ, such as prosecutions or regulatory action by other countries or states. The resulting consequences remain to be seen.

In recent years, there have been some high-profile corporate guilty pleas.[55] The major difference between a guilty plea and an NPA or DPA is that a guilty plea results in a conviction, which generally comes with harsher collateral

51 See *Saena Tech Corp.*, 140 F. Supp. 3d at 31 (discussing the necessity of sufficient deterrent effects); Transcript of Arraignment at 8, *United States v. US Bancorp*, No. 18-CR-150, ECF No. 9 (S.D.N.Y. 22 Feb. 2018) (statement by the court that 'both the interests of deterrence and the interests of just punishment are better served in all or most cases by prosecution of the individuals responsible' and that '[i]f you really want to deter, the way to do it is to make the individuals pay the price for the crimes.').

52 Cf. *US v. HSBC Bank USA, N.A.*, 2013 WL 3306161, at *11 (E.D.N.Y. 1 Jul. 2013) (ordering the parties to file quarterly reports and stating that it will 'notify the parties if, in its view, hearings or other appearances are necessary or appropriate').

53 Lisa O Monaco, Dep. Att'y Gen., Keynote Address at ABA's 36th National Institute on White Collar Crime (28 Oct. 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute ('One immediate area for consideration is whether pretrial diversion — NPAs and DPAs — is appropriate for certain recidivist companies.').

54 Id.

55 For example, in May 2015, Citicorp, JPMorgan Chase & Co., Barclays PLC, Royal Bank of Scotland and UBS all pleaded guilty to felony charges for conspiring to manipulate foreign exchange benchmark rates. DOJ, Press Release, Five Major Banks Agree to Parent-Level Guilty Pleas (20 May 2015), https://www.justice.gov/opa/pr/five-major-banks-agree-parent-level-guilty-pleas; see also Hapoalim (Switzerland) Ltd., Plea Agreement, 20-cr-00262-MKV, ECF No. 5 (S.D.N.Y. 30 Apr. 2020), https://www.justice.gov/opa/pr/israel-s-largest-bank-bank-hapoalim-admits-conspiring-us-taxpayers-hide-assets-and-income#:~:text=Bank%20Hapoalim%20(Switzerland)%20Pleads%20Guilty,the%20United%20States%2C%20Richard%20E; GA Société Générale Acceptance, Plea Agreement, 18-cr-274 (E.D.N.Y. 5 Jun. 2018), https://www.justice.gov/criminal-fraud/file/1072441/download; Rabobank, Plea Agreement, 18-cr-0614 (7 Feb. 2018), https://www.justice.gov/opa/press-release/file/1032101/download; DB Group Servs. Plea Agreement, 3:15CR62 (D. Conn. 23 Apr. 2015), https://www.justice.gov/file/628871/download; BNP Paribas S.A. Order to Cease and Desist (Fed. Reserve Sys. 30 Jun. 2014), https://www.federalreserve.gov/newsevents/press/enforcement/enf20140630a1.pdf; Credit Suisse AG Plea Agreement, 1:14-cr-00188 (E.D. Va. 19 May 2014), https://www.justice.gov/iso/opa/resources/686201451919151694802 2.pdf.

© Law Business Research 2021

regulatory consequences and more significant reputational harm. Such risks for a corporation are significant, especially in a heavily regulated industry – the ramifications can be wide-ranging and unclear. However, there is no indication that guilty pleas will overtake NPAs and DPAs as prosecutors' primary settlement mechanism.

See Section 24.5.3

Regulatory settlements: consent orders and civil NPAs and DPAs 24.4.2

Companies under investigation by federal and state regulators whose enforcement mechanisms are administrative or civil may resolve an investigation by voluntarily entering into a consent order where an institution typically consents to the issuance of a cease-and-desist order or the assessment of a civil monetary penalty, or both. A consent order is a formal enforcement action; it is a public document and, although it may not always be filed, its terms are enforceable in court. Consent orders often vary in the level of detail they provide concerning the wrongdoing, although they are often less detailed than a criminal settlement. A consent cease-and-desist order may oblige the company to undertake remedial measures to correct misconduct and ensure future compliance. The term of the order is usually indefinite. A consent civil monetary penalty assessment obliges the institution to pay a penalty, and the order's terms are fully satisfied by the payment.

Previously, NPAs and DPAs were the exclusive domain of the DOJ, but the SEC,[56] CFTC[57] and state prosecutors[58] have also adopted their use to resolve certain securities law violations. Some have adopted NPAs and DPAs that are similar to their federal criminal counterparts'. For example, the SEC, which is responsible for civil enforcement and administrative actions to enforce the securities laws, has begun to use NPAs and DPAs to resolve cases 'where an entity or person has engaged in misconduct and where the co-operation is

56 See SEC, Office of Chief Counsel, Enforcement Manual § 6.2.2, Deferred Prosecution Agreements (28 Nov. 2017); SEC, Office of Chief Counsel, Enforcement Manual § 6.2.3, Non-Prosecution Agreements (28 Nov. 2017); SEC, Press Release, SEC Announces Initiative to Encourage Individuals and Companies to Cooperate and Assist in Investigations (13 Jan. 2010), http://www.sec.gov/news/press/2010/2010-6.htm (announcing Cooperation Initiative, including co-operation agreements, DPAs and NPAs).

57 See CFTC, Division of Enforcement, Enforcement Manual § 7.2, Cooperation Tools (20 May 2020), https://www.cftc.gov/media/1966/The%2520CFTC%2520Division%2520of%2520Enforcement%2520-%2520Enforcement%2520Manual/download.

58 See Memorandum from Daniel R Alonso, Chief Assistant District Attorney, District Attorney of the County of New York, Considerations in Charging Organizations § II.1 (27 May 2010), https://www.manhattanda.org/wp-content/themes/dany/files/Considerations%20in%20Charging%20Organizations.pdf ('In certain circumstances, it may be appropriate to enter into a deferred prosecution agreement ("DPA") or non-prosecution agreement ("NPA") with an organization.').

© Law Business Research 2021

extraordinary, but the circumstances call for a measure of accountability'.[59] NPAs and DPAs, however, remain uncommon for civil enforcement actions by the SEC.[60] From 2017 to the time of writing in 2021, the SEC had not entered into any NPAs or DPAs.[61]

24.5 Key settlement terms

Whether negotiating a settlement agreement in the criminal or regulatory context, many common principles come into play. To facilitate a successful negotiation, a company must have a comprehensive understanding of (1) benchmark terms for historical settlements regarding similar misconduct, (2) those terms that are most significant to the company and (3) any distinguishing factors in the matter at issue that encourage terms less severe than the benchmarks.

24.5.1 Monetary penalties

Nearly all corporate settlements with US authorities include some form of monetary penalty. The form largely depends on the US authority and its practices. Typically, monetary penalties in regulatory settlements consist of a civil monetary penalty. Disgorgement of profits or restitution to harmed parties may also be required.[62]

---

59 Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute, The SEC's Cooperation Program: Reflections on Five Years of Experience (13 Mar. 2015), https://www.sec.gov/news/speech/sec-cooperation-program.html.

60 Id. ('[T]hey have been a relatively limited part of our practice. I think this is appropriate and should continue to be the case.'); see also SEC, Office of Chief Counsel, Enforcement Manual § 6.2.3, Non-Prosecution Agreements (28 Nov. 2017) ('A non-prosecution agreement is a written agreement . . . entered in limited and appropriate circumstances.').

61 See 2021 Mid-Year Update on Corporate Non-Prosecution Agreements and Deferred Prosecution Agreements (22 Jul. 2021), https://www.gibsondunn.com/2021-mid-year-update-on-corporate-non-prosecution-agreements-and-deferred-prosecution-agreements/ ('The SEC has not entered into any NPAs or DPAs in 2021'); 2020 Year-End Update on Corporate Non-Prosecution Agreements and Deferred Prosecution Agreements (19 Jan. 2021), https://www.gibsondunn.com/2020-year-end-update-on-corporate-non-prosecution-agreements-and-deferred-prosecution-agreements/ ('The SEC has not entered into any NPAs or DPAs in 2020')); 2019 Year-End Update on Corporate Non-Prosecution Agreements and Deferred Prosecution Agreements (8 Jan. 2020), https://www.gibsondunn.com/2019-year-end-npa-dpa-update/#_ednref8 ('The SEC has not entered into any NPAs or DPAs in 2019.'); 2018 Mid-Year Update on Corporate Non-Prosecution Agreements (NPAs) and Deferred Prosecution Agreements (DPAs) (10 Jul. 2018), https://www.gibsondunn.com/2018-mid-year-npa-dpa-update/ ('[A]s in 2017, the SEC has not entered into any NPAs or DPAs in 2018.').

62 Forfeiture, the seizure of assets that comprised the proceeds of the wrongdoing, or were used to facilitate it, is rarely used in regulatory actions against business entities even when available, because the government is generally reluctant to seize property related to an

© Law Business Research 2021

Generally, the factors that US authorities consider in determining monetary penalties mirror those used to determine whether to bring charges against the corporation in the first place, including the nature of the offence, the company's timely and voluntary disclosure of wrongdoing, and the company's remedial actions. For example, the SEC considers two principal factors in determining monetary penalties: the presence or absence of a direct and material benefit to the corporation itself as a result of the violation and the degree to which the penalty will recompense or further harm the injured shareholders.[63] The SEC will also consider factors such as deterring the conduct, the extent of the injury, any complicity on the part of the corporation, the intent of the individuals committing the wrong, the difficulty in detecting that particular type of wrongdoing, any remedial steps taken by the corporation and the extent of its co-operation.[64]

In June 2017, the US Supreme Court issued a seemingly consequential decision that could have diminished the SEC's leverage in settlement negotiations. In *Kokesh v. SEC*,[65] the Supreme Court held that a five-year statute of limitations applies to SEC enforcement actions seeking disgorgement.[66] *Kokesh*

---

ongoing business. See Justice Manual § 9-111.124, Business Seizures (updated Jan. 2020) ('Due to the complexities of seizing an ongoing business and the potential for substantial losses from such a seizure, a United States Attorney's Office must consult with the [Money Laundering and Asset Recovery Section] prior to initiating a forfeiture action against, or seeking the seizure of, or moving to restrain an ongoing business.'). Restitution, the compensation of individuals harmed by illegal conduct, is also rarely a part of any settlement. In particularly complex cases involving many different classes of individuals that may have been harmed, calculation of restitution may be especially difficult, and a corporation may find the government amenable to not seeking restitution in its settlement, with the understanding that compensation of harmed individuals is more efficiently and accurately handled through related civil litigation. See 18 U.S.C. § 3663A(c)(3).

63 SEC Release No. 2006-4, Statement of the Securities and Exchange Commission Concerning Financial Penalties (4 Jan. 2006), https://www.sec.gov/news/press/2006-4.htm. See also Caroline A Crenshaw, SEC Commissioner, Speech: Moving Forward Together – Enforcement for Everyone (9 Mar. 2021), https://www.sec.gov/news/speech/crenshaw-moving-forward-together ('Since [2006], when assessing penalties, the Commission has looked at whether a corporation's shareholders benefited from misconduct, or whether they will be harmed by the assessment of a penalty because the costs may be passed on to shareholders. This myopic approach is flawed and the reason why we need to make a change.').

64 Id.

65 137 S. Ct. 1635 (2017).

66 Id. at 1645. Prior to this ruling, the SEC relied disproportionately on disgorgement penalties. In 2015, the SEC obtained US$3 billion in disgorgement payments and US$1.2 billion in other civil monetary penalties. See SEC, 'Select SEC & Market Data: Fiscal 2015' (2016), https://www.sec.gov/reportspubs/select-sec-and-market-data/secstats2015.pdf. In FY 2016, the SEC obtained US$2.8 billion in disgorgement payments and US$1.3 billion in other civil monetary penalties. See SEC, Division of Enforcement, Annual Report: A Look Back at Fiscal Year 2017 (15 Nov. 2017), https://www.sec.gov/files/enforcement-annual-report-2017.pdf. In FY 2017, the disproportionality was more stark, with US$3 billion in disgorgement payments and US$832 million in other civil monetary penalties. Id.

© Law Business Research 2021

also raised the question of whether the Court would, in fact, recognise disgorgement as an available remedy in SEC enforcement proceedings.[67] In June 2020, the Court addressed this issue in *Liu v. SEC*,[68] upholding the use of disgorgement by the SEC so long as a disgorgement award 'does not exceed a wrongdoer's net profits'.[69] Looking at the numbers alone, *Kokesh* does not seem to have greatly affected disgorgement in SEC enforcement actions.[70] In response to the uncertain impact of *Liu*, however, the SEC plans to continue 'changes in the balance between the penalties and disgorgement', and may thus 'recommend higher penalties in some cases where the statutory scheme permits'.[71]

As to criminal monetary penalties, the DOJ announced in 2019 a written policy formalising how the Criminal Division should consider a company's argument that it is financially unable to pay an otherwise appropriate penalty.[72] Under the policy, which aims to promote transparency around corporate penalties, the parties must first agree on the form of a corporate criminal resolution and the otherwise appropriate monetary penalty in the absence of the inability-to-pay considerations. The company must then complete an 11-point questionnaire, which requires the disclosure of, among other things, cash-flow projections, federal income tax returns for the past five years, operating budgets, acquisition or divestiture plans, encumbered assets and payments to the business's highest-earning executives.[73] DOJ lawyers are then directed to consider that information in light of statutory sentencing factors, the US Sentencing Guidelines, and the Justice Manual's principles regarding the consideration of collateral consequences in resolving a corporate criminal case.[74]

See Chapter 26 on fines, disgorgement, etc.

67 Id. at 1642, n. 3 ('Nothing in this opinion should be interpreted as an opinion on whether courts possess authority to order disgorgement in SEC enforcement proceedings or on whether courts have properly applied disgorgement principles in this context. The sole question presented in this case is whether disgorgement, as applied in SEC enforcement actions, is subject to § 2462's limitations period.').

68 140 S. Ct. 1936 (2020).

69 Id. at 1940.

70 Disgorgement recoveries increased from US$2.8 billion in FY 2016 to US$3 billion in FY 2017, before dipping to US$2.5 billion in FY 2018. See SEC, Division of Enforcement, 2018 Annual Report at 11 (2 Nov. 2018), https://www.sec.gov/files/enforcement-annual-report-2018.pdf. In FY 2019, however, disgorgement recoveries increased to US$3.2 billion, and despite the covid-19 pandemic, disgorgement reached $3.589 billion in FY 2020. See SEC, Division of Enforcement, 2019 Annual Report at 16 (6 Nov. 2019), https://www.sec.gov/files/enforcement-annual-report-2019.pdf; SEC, Division of Enforcement, 2020 Annual Report, at 17 (2 Nov. 2020), https://www.sec.gov/files/enforcement-annual-report-2020.pdf.

71 SEC, Division of Enforcement, 2020 Annual Report at 7 (2 Nov. 2020), https://www.sec.gov/files/enforcement-annual-report-2020.pdf.

72 Memorandum from Brian A Benczkowski, Assistant Att'y Gen., US Dep't of Justice, Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty (8 Oct. 2019), https://www.justice.gov/opa/speech/file/1207576/download.

73 Id. at Attachment A.

74 Id. at 1.

© Law Business Research 2021

Continuing obligations 24.5.2

In addition to monetary penalties, settlement agreements will often include other continuing obligations. In particular, settlement agreements almost always contain language stating that the company will commit to undertake remedial efforts, such as the enhancement of its compliance programmes or an obligation to report potential violations of law in the future. To ensure ongoing compliance and satisfactory remedial efforts, government agencies may require the use of corporate monitors to keep corporations accountable.

A potentially substantial obligation in corporate settlements is the imposition of a monitor to oversee a company's compliance with a settlement agreement and report back to the government on the company's progress. The requirement of an independent monitor was common for DPAs and NPAs, but self-monitoring and reporting became more standard in settlement agreements. Recently, there appears to be a resurgence of the imposition of outside monitors.[75] In October 2021, the DOJ made clear that 'there is no default presumption against corporate monitors'.[76] The DOJ 'is free to require the imposition of independent monitors whenever it is appropriate to do so in order to satisfy our prosecutors that a company is living up to its compliance and disclosure obligations under the DPA or NPA'.[77] In an attempt at greater transparency, the DOJ issued guidance in October 2018 for the selection of monitors in criminal matters.[78]

See Chapter 33 on monitorships

Monitorships, which may last for a number of years, are a financial and functional burden on a company. Monitorships can be draining in terms of the cost of retaining the monitor itself, the costs required to implement recommended reforms, the cost of staffing and maintaining an internal team to work

75 In April 2020, the DOJ published for the first time a list identifying all active corporate monitors by companies as part of criminal resolutions. See DOJ, List of Independent Compliance Monitors for Active Fraud Section Monitorships, https://www.justice.gov/criminal-fraud/strategy-policy-and-training-unit/monitorships (last visited 26 Aug. 2021). As of August 2021, the DOJ Fraud Section had seven active monitors: one appointed in 2016; one in 2017; three in 2019; one in 2020; and one in 2021.

76 Lisa O Monaco, Dep. Att'y Gen., Keynote Address at ABA's 36th National Institute on White Collar Crime (28 Oct. 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

77 Id.

78 Brian A Benczkowski, Memorandum from the US Dep't of Justice on Selection of Monitors in Criminal Division Matters (11 Oct. 2018), https://www.justice.gov/opa/speech/file/1100531/download. The memorandum instructs DOJ attorneys to consider, among other factors, whether '(a) the underlying misconduct involved the manipulation of corporate books and records or the exploitation of an inadequate compliance program or internal control systems, (b) the misconduct at issue was pervasive across the business organization or approved or facilitated by senior management, (c) the corporation has made significant investments in, and improvements to, its corporate compliance program and internal control systems, and (d) remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future'. Id. at 2.

© Law Business Research 2021

closely with the monitor and the disruption to the company's business and management. Another important consideration when contemplating a monitorship as a term of settlement is that monitors are generally given broad access to the corporation's files, outside the protection of an attorney–client relationship. This lack of attorney–client relationship can pose a risk of further legal exposure for the company. Given that a monitor is tasked with reviewing the corporation's practices, and reporting the findings of the review to relevant authorities, it is possible that the monitor will identify and be obliged to disclose additional violations of law to relevant authorities. In addition, once a monitor's reports are submitted to the relevant authorities, those reports and any documents contained in them can be subject to Freedom of Information Act requests, which may create additional exposure in follow-on civil litigation.[79]

Given the substantial expense and disruption caused by a monitorship, it is in a corporation's interest to try and avoid the imposition of a monitor – especially in instances where corporate culpability is relatively low and the company has already undertaken substantial remedial efforts. The most effective way for a company to avoid the imposition of a monitor continues to be to voluntarily report its misconduct, to co-operate fully with the government's resulting investigation and to demonstrate to the government that the company has already undertaken a comprehensive remediation plan. Where a monitor is imposed, a corporation can mitigate the disruption by negotiating the monitor's duration of assignment, scope of responsibility, decision-making capacity and accessibility to corporate files.

24.5.3 Collateral consequences

A criminal or regulatory settlement can also trigger a number of collateral consequences, which can vary depending on the types of violations the settlement covers and the industry of the affected entity. For example, a guilty plea for a bank could mean the loss of its financial holding company status and federal deposit insurance, the appointment of a receiver or conservator, and, for foreign banks, the potential termination of offices in the United States. A guilty plea for a broker-dealer could mean automatic loss of broker-dealer registration, a bar from acting as a registered investment adviser, and revocation of its status as a well-known seasoned issuer. A guilty plea for a corporation could also result in, among other things, disqualification from membership of certain self-regulatory organisations, a temporary or permanent bar from

79 See *New York Times Co.*, 2021 WL 371784, at *8 (S.D.N.Y. 3 Feb. 2021) (ordering in camera review of a monitor report after rejecting 'Intervenor's and Defendant's argument that all information about VW's compliance program is itself commercial and exempt under Exemption 4' but finding that 'Defendant and Intervenor have sufficiently established that the Report likely contains some commercial information and that such information is "confidential".'); *100Reporters LLC v. United States Dep't of Justice*, 316 F. Supp. 3d 124 (D.D.C. 2018) (holding that the DOJ's attempts to withhold parts of a monitor's report under FOIA Exemptions 4, 5, 6 and 7(C) were overly broad).

© Law Business Research 2021

participation in federal procurement contracts (debarment), or loss of state licences. Compounding these difficulties, many of the collateral consequences that arise upon conviction travel within a corporation's legal structure, so that even regulated businesses that were not involved in the offence can be subject to licence revocations, loss of securities law safe harbours and other consequences.

Corporations may need to seek waivers or exemptions from multiple regulators including the SEC, the CFTC, the Federal Reserve, the Department of Labor and the Financial Industry Regulatory Authority to allow them to continue engaging in the affected business activities, a process that should be planned well in advance of settlement. Each regulator may have more than one relevant exemption.[80] The company will therefore need to assess the relevant regulations for each authority that oversees the company's activities. The permutations of collateral consequences are many and depend on the form of the settlement (e.g., DPA, NPA, guilty plea, conviction or consent order) or even the nature of the offence.[81] In addition to automatic disqualifications, there is a wide array of discretionary actions available to regulators for which waivers or exemptions could be sought.[82]

The method of receiving a waiver or exemption from these collateral consequences depends on the agency. For the SEC, a corporation requests an exemption from the SEC Staff, which can either make a recommendation to the Commission or act directly on the application with delegated authority from the Commission.[83] The SEC generally grants a waiver under a finding of

80 The SEC has many, including: (1) status as a well-known seasoned issuer (WKSI); (2) status under § 9(a) of the 1940 Act as an investment adviser, depositor or principal underwriter of registered investment companies; and (3) exemptions from certain capital-raising restrictions, under Regulations A and D. See also generally Richard A Rosen and David S Huntington, 'Waivers from the Automatic Disqualification Provisions of the Federal Securities Laws', 29:8 *Insights: The Corp. & Sec. Law Advisor* at 2 (8 Aug. 2015) (cataloguing various SEC waivers).

81 Naturally, criminal convictions have much more severe consequences than a DPA, NPA or administrative consent order. For instance, § 9(a) of the Investment Company Act of 1940 automatically bars an entity from acting as investment adviser or providing certain other services to registered investment companies if that entity or an affiliated entity has been convicted within the past ten years of any felony or misdemeanour arising out of the conduct of the business of a bank. 15 U.S.C. § 80a-9(a)(1).

82 For example, under § 15(b)(4) of the Securities Exchange Act, the SEC has the discretion after a conviction to suspend or revoke the registration of a broker-dealer if it finds, after notice and comment, that it is in the public interest. See 15 U.S.C. § 78o(b)(4)(B).

83 In July 2019, SEC Chairman Jay Clayton announced that the Commission would allow companies to make offers of settlement contingent on the receipt of requested disqualification waivers. SEC Chairman Jay Clayton, Statement Regarding Offers of Settlement (3 Jul. 2019), https://www.sec.gov/news/public-statement/clayton-statement-regarding-offers-settlement ('[A] settling entity can request that the Commission consider an offer of settlement that simultaneously addresses both the underlying enforcement action and any related collateral disqualifications.'). In February 2021, under a new US presidential administration, Acting Chair Allison Herren Lee returned to the SEC's

© Law Business Research 2021

'good cause'.[84] In contrast, the Department of Labor, in granting exemptions for qualified professional asset manager status, engages in a formal rule-making process, including a public notice and comment period.[85] The Federal Reserve, which can take a range of discretionary actions, generally engages in a more informal regulatory-relations dialogue when considering the collateral consequences of a significant settlement.

Timing is critical for the waiver process, because a company will need to ensure that there is no gap in its licences and statuses. Complicating matters, regulators often take different views as to when statutory disqualifications based on convictions or settlements commence. The SEC views 'conviction' as entry into a guilty plea, so any relevant SEC waivers need to be lined up before then. In contrast, the Department of Labor says that conviction is at sentencing, which can take place well after the entry of the guilty plea. For this reason, sentencing after the entry of a guilty plea can be delayed for the purpose of obtaining the necessary exemption from the Department of Labor.[86]

24.5.4 Admissions and follow-on civil litigation

With increasing frequency, as a condition of settlement, government authorities are requiring corporations to make factual or legal admissions, or both. In addition to the reputational impact and collateral consequences that such admissions can impose on a corporation, admissions can expose a company to significant liability in follow-on civil litigation. Plaintiffs may be able to rely on factual or legal admissions in settlement agreements, including DPAs and NPAs, to support a complaint, and may attempt to introduce them as evidence later.[87] A corporation will have a stronger argument that an administrative

---

'long-standing practice' of not making settlement conditional on receipt of requested waivers. Acting SEC Chair Allison Herren Lee, Statement on Contingent Settlement Offers (11 Feb. 2021), https://www.sec.gov/news/public-statement/lee-statement-contingent-settlement-offers-021121 ([T]the Division of Enforcement will no longer recommend to the Commission a settlement offer that is conditioned on granting a waiver.').

84 17 C.F.R. § 230.405, Ineligible Issuer § 2 ('An issuer shall not be an ineligible issuer if the Commission determines, upon a showing of good cause, that it is not necessary under the circumstances that the issuer be considered an ineligible issuer.').

85 29 C.F.R. pt. 2570, subpt. B.

86 For example, in the set of plea agreements associated with manipulating foreign exchange benchmark rates, there was a term that the United States would support any motion or request to delay sentencing until the Department of Labor had issued a ruling on the request for exemption. Barclays Plea Agreement ¶ 12(e), Case No. 3:15-cr-00077, ECF No. 6 (D. Conn. 20 May 2015), https://www.justice.gov/file/440481/download; UBS Plea Agreement ¶ 28, Case No. 3:15-cr-00076, ECF No. 6 (D. Conn. 20 May 2015), https://www.justice.gov/file/440521/download.

87 For example, *In re Veon Ltd. Sec. Litig.*, 2018 WL 4168958, at *1 (S.D.N.Y. 30 Aug. 2018) ('Plaintiffs' complaint also relies heavily on a criminal complaint and Deferred Prosecution Agreement'); *Menaldi v. Och-Ziff Capital Mgmt. Grp. LLC*, 277 F. Supp. 3d 500, 509 (S.D.N.Y. 2017) ('The key difference between the factual allegations in the Old Complaint and those

© Law Business Research 2021

consent order does not represent an adjudication and cannot be relied on in a complaint although litigation on the issue has been met with mixed results.[88]

A corporation entering into a settlement agreement ideally should, to the extent possible, try to neither admit nor deny the charges, in which case the findings of the order are less likely to be able to be used against it. In the event that a corporation is unable to do so, a company should strategically negotiate for narrowly tailored factual statements and flexible language to enable it to defend itself in follow-on civil litigation. In particular, admitting to a generalised violation of law may be less likely to have future adverse consequences than admission of a specific legal violation that shares elements of claims that could be brought in follow-on civil litigation.

Furthermore, a corporation should be aware that settlement agreements that dictate that the corporation cannot contradict the findings of facts can

---

in the New Complaint is the level of detail regarding Och–Ziff's dubious dealings in Africa. Of great help are the DPA and the SEC Settlement, both of which are incorporated into the New Complaint.'); *7 W. 57th St. Realty Co., LLC v. Citigroup, Inc.*, 2015 WL 1514539, at *1 n. 1 (S.D.N.Y. 31 Mar. 2015), aff'd, 771 F. App'x 498 (2d Cir. 2019) ('[T]he Court has also considered documents that are incorporated into the Amended Complaint by reference, including non-prosecution and deferred prosecution agreements that certain Defendants entered into with the United States Department of Justice').

88 For example, the Second Circuit has held that 'a consent judgment between a federal agency and a private corporation which is not the result of an actual adjudication of any of the issues . . . can not be used as evidence in subsequent litigation between that corporation and another party'. *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887, 893 (2d Cir. 1976); see also *Waterford Tp. Police & Fire Ret. Sys. v. Smithtown Bancorp, Inc.*, 2014 WL 3569338 (E.D.N.Y. 18 Jul. 2014) (striking from complaint references to consent agreements with the Federal Deposit Insurance Corporation and the New York Banking Department); *In re Rough Rice Commodity Litig.*, 2012 WL 473091, at *5 (N.D. Ill. 9 Feb. 2012) ('Under *Lipsky* and its progeny, the findings of the CFTC in its Order are not a sufficient basis for a manipulation claim.'); *In re Platinum & Palladium Commodities Litig.*, 828 F. Supp. 2d 588 (S.D.N.Y. 13 Sep. 2011) (striking from complaint references to CFTC's findings of fact contained in an administrative consent order). But see *In re Herbal Supplements Mktg. & Sales Practices Litig.*, 2017 WL 2215025, at *6 (N.D. Ill. 19 May 2017) (reading *Lipsky* narrowly and as 'nonbinding authority' with limited application to materials from the New York State Office of the Attorney General); *Tobia v. United Grp. of Cos., Inc.*, 2016 WL 5417824, at *3 (N.D.N.Y. 22 Sep. 2016) (holding that while the SEC complaint and consent order are inadmissible to prove liability under *Lipsky*, the allegations and findings enumerated in the SEC complaint are not made inadmissible merely by virtue of their inclusion therein); *In re OSG Sec. Litig.*, 12 F. Supp. 3d 619, 621 (S.D.N.Y. 2014) ('*Lipsky* did not hold that a complaint may never reference allegations from a separate proceeding under any circumstances.') (collecting cases); *In re Bear Stearns Mortg. Pass-Through Certificates Litig.*, 851 F. Supp. 2d 746, 768 n. 24 (S.D.N.Y. 2012) ('[S]ome courts in this district have stretched the holding in *Lipsky* to mean that any portion of a pleading that relies on unadjudicated allegations in another complaint is immaterial under Rule 12(f). Neither Circuit precedent nor logic supports such an absolute rule.') (citation omitted).

© Law Business Research 2021

restrict the corporation's positions in follow-on civil litigation.[89] Because any statement that could be viewed by the government as contradictory to the facts of the agreement may then be seen as a breach – thereby reviving a prosecutorial or regulatory action[90] – it is important that such agreements, at a minimum, contain exceptions that allow a company to take good-faith positions in follow-on civil litigation or that allow a company to cure a potential breach.[91]

24.6 Resolving parallel investigations

24.6.1 Other domestic authorities

Most large-scale investigations of corporations involve a number of government agencies from federal and state governments, both prosecutorial and regulatory. The degree of coordination among these agencies varies case by case,

89 See, e.g., *In re Bank Hapoalim B.M.*, DPA, tax evasion (30 Apr. 2020), https://www.justice.gov/opa/press-release/file/1275081/download ('BHBM admits and stipulates that the facts set forth in the Statement of Facts . . . are true and accurate. In sum, BHBM admits that it is responsible under US law for the federal criminal violations charged in the Information and set forth in the Statement of Facts as a result of the acts of its officers, directors, employees and agents.'); SEC Release No. 88295, Order Instituting Cease-and-Desist Proceedings, *In the Matter of Wells Fargo Clearing Service, LLC* (27 Feb. 2020), https://www.sec.gov/litigation/admin/2020/34-88295.pdf ('Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over them and the subject matter of these proceedings, which are admitted.'); cf. SEC Release No. 90875, Order Instituting Cease-and-Desist Proceedings, *In the Matter of Deutsche Bank AG* (8 Jan. 2021), https://www.sec.gov/litigation/admin/2021/34-90875.pdf (clarifying that '[t]he findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.').

90 See *United States v. Goldfarb*, 2012 WL 3860756 (N.D. Cal. 5 Sep. 2012) (finding that defendants were in material breach of their DPA and thus denying defendants' motion to dismiss criminal charges).

91 See, e.g., *In re Wells Fargo*, DPA ¶ 5 (20 Feb. 2020), https://www.justice.gov/usao-cdca/press-release/file/1251336/download ('If the USAOs determine that Wells Fargo has made a public statement contradicting its acceptance of responsibility . . . , the USAOs shall so notify Wells Fargo. Thereafter, Wells Fargo may avoid a breach of this Agreement by publicly repudiating the statement within five days after such notification. Wells Fargo shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Statement of Facts provided that such defenses and claims do not contradict, in whole or in part, any statement contained in the attached Statement of Facts.'); *In the Matter of Citibank, N.A.*, CFTC Docket No. 16-16 at 26 (25 May 2016), www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcitibankisdaorder052516.pdf. ('Respondent agrees that neither it nor any of its successors and assigns, agents, or employees under its authority of control shall take any action or make any public statement denying directly or indirectly, any findings or conclusions in this Order or creating, or tending to create, the impression that this Order is without a factual basis; provided, however, that nothing in this provision shall affect Respondent's (i) testimonial obligations, or (ii) right to take positions in other proceedings to which the Commission is not a party.').

© Law Business Research 2021

and coordinating with multiple agencies can be challenging. However, there can be benefits to coordinated settlements, including closure for the company, enhanced legal certainty and the avoidance of unnecessary duplication, or undue burdens of disclosure.[92] In addition, because the settlement announcements can occur on a single day, a company may be better able to control the release of information concerning the settlements and thereby limit the effect of any harmful disclosures on the market.[93] There is a distinct trend towards more multi-agency settlements, as agencies increase collaboration, even across

92 In May 2018, the DOJ announced a new policy encouraging coordination by the DOJ with other US and international law enforcement agencies conducting investigations of the same conduct to avoid 'disproportionate enforcement of laws by multiple authorities'. DOJ, Dep. Att'y Gen. Rod Rosenstein Delivers Remarks to the New York City Bar White Collar Crime Committee (Remarks as prepared for delivery) (9 May 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar. In June 2018, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation released a 'Policy Statement on Interagency Notification of Formal Enforcement Actions.' 83 Fed. Reg. 113 at 27371–72 (12 Jun. 2018), https://www.occ.gov/news-issuances/federal-register/2018/83fr27371.pdf. The statement requires the agencies to notify each other of enforcement actions against financial institutions, especially when the action they are pursuing involves the interests of another agency. Id. at 27372. If two or more of the agencies consider bringing complementary actions, they 'should coordinate the preparation, processing, presentation, potential penalties, service, and follow-up' of the enforcement action. Id.

93 For example, in January 2018, the CFTC and DOJ announced on the same day eight coordinated 'anti-spoofing' enforcement actions. See US CFTC, Press Release, CFTC Files Eight Anti-Spoofing Enforcement Actions against Three Banks (Deutsche Bank, HSBC & UBS) & Six Individuals (29 Jan. 2018), https://www.cftc.gov/PressRoom/PressReleases/pr7681-18; DOJ, Press Release, Eight Individuals Charged with Deceptive Trading Practices Executed on US Commodities Markets (29 Jan. 2018), https://www.justice.gov/opa/pr/eight-individuals-charged-deceptive-trading-practices-executed-us-commodities-markets; see also SEC, Press Release, JPMorgan Chase Agrees to Pay $200 Million and Admits Wrongdoing to Settle SEC Charges (19 Sep. 2013), https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539819965 ('As part of a coordinated global settlement, three other agencies also announced settlements with JPMorgan today: the UK Financial Conduct Authority, the Federal Reserve, and the Office of the Comptroller of the Currency.'); SEC, Press Release, Standard Bank to Pay $4.2 Million to Settle SEC Charges (20 Nov. 2015), https://www.sec.gov/news/pressrelease/2015-268.html. Media criticism may also be diffused through coordinated settlements among companies. See DOJ, Press Release, Five Major Banks Agree to Parent-Level Guilty Pleas' (20 May 2015), https://www.justice.gov/opa/pr/five-major-banks-agree-parent-level-guilty-pleas (global settlement of claims against five banks – Citicorp, JPMorgan Chase & Co., Barclays PLC, The Royal Bank of Scotland plc, and UBS AG – involving the DOJ, the Federal Reserve, CFTC, and the New York State Department of Financial Services in the United States, and the Financial Conduct Authority in the United Kingdom).

© Law Business Research 2021

borders.[94] In 2018, the DOJ announced a policy intended to encourage coordination between it and other enforcement agencies and to discourage the disproportionate enforcement of laws by multiple authorities.[95] Among other things, the policy sets forth factors that DOJ attorneys may evaluate in determining whether multiple penalties serve the interests of justice in a particular case, including the egregiousness of the wrongdoing and the adequacy and timeliness of a company's disclosures and co-operation.[96]

94 In recent years, the DOJ has coordinated with the SEC and CFTC in spoofing enforcement. This coordination extends to interagency 'task forces', such as the establishment in July 2018 under the Trump administration of a task force on market integrity and consumer fraud that, among other things, combats corporate fraud that victimises the general public and the government. Other examples of multi-agency settlements include foreign corruption. See Press Release, DOJ, Vitol Inc. Agrees to Pay over $135 Million to Resolve Foreign Bribery Case (Dec. 3, 2020), https://www.justice.gov/opa/pr/vitol-inc-agrees-pay-over-135-million-resolve-foreign-bribery-case; Press Release, CFTC, CFTC Orders Vitol Inc. to Pay $95.7 Million for Corruption-Based Fraud and Attempted Manipulation (3 Dec. 2020), https://www.cftc.gov/PressRoom/PressReleases/8326-20 (first CFTC action involving foreign corruption). See also *In re Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Products Liability Litigation*, 3:15-mc-02672-CRB (N.D. Cal. 17 May 2017) (consent decree with the DOJ, on behalf of the EPA and stipulated order for permanent injunction and monetary judgment for the FTC); *SEC v. Teva Pharmaceutical Industries, Ltd.*, 1:16-cv-25298 (S.D. Fla. 22 Dec. 2016), https://www.sec.gov/litigation/litreleases/2016/lr23708.htm (DPA with the DOJ and interest and disgorgement payments to the SEC in connection with civil and criminal violations of the Foreign Corrupt Practices Act); SEC Release No. 78989, Order Instituting Administrative and Cease-and-Desist Proceedings (29 Sep. 2016) (Och-Ziff DPA with the DOJ and interest and disgorgement payments to the SEC to resolve criminal charges arising out of bribes paid to public officials in the Democratic Republic of Congo and Libya), https://www.sec.gov/litigation/admin/2016/34-78989.pdf; Commerzbank AG Plea Agreement (D.D.C. 12 Mar. 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf (DPAs with the DOJ and DANY and consent orders with OCC and FinCEN); JPMorgan Chase Bank, N.A. Deferred Prosecution Agreement (S.D.N.Y. 6 Jan. 2014), https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/JPMC%20DPA%20Packet%20%28Fully%20Executed%20w%20Exhibits%29.pdf (DPA with the DOJ and consent orders with the Federal Reserve, OFAC and NYDFS); SEC Release No. 9453, Order Instituting Cease-and-Desist Proceedings, In the Matter of TD Bank, N.A. (23 Sep. 2013), https://www.sec.gov/litigation/admin/2013/33-9453.pdf (consent orders with the OCC and FinCEN and cease-and-desist order with SEC).

95 DOJ, Dep. Att'y Gen. Rod Rosenstein Delivers Remarks to the New York City Bar White Collar Crime Committee (Remarks as prepared for delivery) (9 May 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

96 Id.

© Law Business Research 2021

Foreign authorities 24.6.2

Owing at least in part to the internationalisation of enforcement, the global nature of modern-day securities frauds, increased regulatory activity on the state level and the increased complexity of the markets,[97] regulatory investigations today tend to involve a variety of authorities.[98] Thus, a corporation must carefully evaluate whether a settlement with certain authorities should be postponed until a global resolution can be reached. Coordinated global settlements often afford the company the opportunity to predict and prevent excessive, cumulative or unnecessary monetary penalties, continuing obligations and collateral consequences.[99]

97 Mary Jo White, SEC Chair, Speech at the New York Bar Association's Third Annual White Collar Crime Institute, 'Three Key Pressure Points in the Current Enforcement Environment' (19 May 2014), https://www.sec.gov/news/speech/2014-spch051914mjw.html.

98 Many of the highest-profile settlements have been the result of cooperative efforts between US and foreign regulators. Indeed, the 10 largest FCPA settlements with the US were the result of co-operative investigations between US and foreign authorities: Odebrecht S.A. (US$3.56 billion), The Goldman Sachs Group, Inc. (US$2.62 billion), Airbus SE (US$2.09 billion), Petróleo Brasileiro S.A. (US$1.79 billion), Telefonaktiebolaget LM Ericsson (US$1.06 billion), Telia Company AB (US$965.6 million), Mobile TeleSystems PJSC (US$850.0 million), Siemens Aktiengesellschaft (US$800.0 million), VimpelCom Ltd (US$795.3 million) and Alstom S.A. (US$772.3 million).

99 For example, in January 2020, as part of the largest global foreign bribery resolution, Airbus SE, a global provider of aircraft based in France, paid more than US$3.9 billion to resolve foreign bribery charges. DOJ, Press Release, Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case (31 Jan. 2020), https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case. The agreement included the payment of US$527 million and €50 million in forfeiture to the DOJ, with US$1,797,490,796 credited to France's Parquet National Financier's separate record high recovery of €2.1 billion. See Airbus DPA ¶ 8, 20-cr-00021, ECF No. 8 (D.D.C. 31 Jan. 2020). Airbus also paid €991 million under a DPA with the UK's Serious Fraud Office. See 'SFO Enters into €991m Deferred Prosecution Agreement with Airbus as Part of a €3.6bn Global Resolution' (31 Jan. 2020), https://www.sfo.gov.uk/2020/01/31/sfo-enters-into-e991m-deferred-prosecution-agreement-with-airbus-as-part-of-a-e3-6bn-global-resolution/. In December 2016, Odebrecht entered a plea agreement with the DOJ, providing that 'the United States will credit the amount that Odebrecht pays to Brazil and Switzerland over the full term of their respective agreements.' DOJ, Press Release, 'Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History' (21 Dec. 2016), https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve. And, as part of a global settlement with Embraer to resolve alleged FCPA violations, the SEC announced that 'Embraer may receive up to a $20 million credit depending on the amount of disgorgement it will pay to Brazilian authorities in a parallel civil proceeding in Brazil.' SEC, Press Release, 'Embraer Paying $205 Million to Settle FCPA Charges' (24 Oct. 2016), https://www.sec.gov/news/pressrelease/2016-224.html.

© Law Business Research 2021

25

Fines, Disgorgement, Injunctions, Debarment: The UK Perspective

Tom Epps, Marie Kavanagh, Andrew Love, Julia Maskell and Benjamin Sharrock[1]

25.1 Criminal financial penalties

Financial penalties for corporate and individual fraud, bribery and money laundering offences are determined in accordance with relevant legislation and the sentencing guidelines issued by the Sentencing Council.[2] For corporates, the relevant guideline is 'Corporate Offenders: fraud, bribery and money laundering' (the Guideline).[3] The Guideline applies to corporates sentenced on or after 1 October 2014, regardless of the date of the offence, and must be followed by the court unless it would be contrary to the interests of justice to do so.[4]

In applying sentencing guidelines to offences prosecuted under legislation that pre-dates them, the court may reflect 'modern attitudes' to historic offences and make allowance for any change in maximum sentence for that particular

1 Tom Epps is a partner, and Marie Kavanagh, Andrew Love, Julia Maskell and Benjamin Sharrock are associates, at Cooley LLP. The authors wish to acknowledge the contributions of Kelly Hagedorn, Robert Dalling and Matthew Worby, the authors of the corresponding chapter in the previous edition of this Guide, on which this chapter is partly based.

2 The Sentencing Council publishes separate guidelines for the magistrates' and Crown courts. Many guidelines are offence-specific, but there are also overarching guidelines on various topics, including a General Guideline with Overarching Principles, effective from 1 October 2019, to be used in conjunction with the specific guideline or where no offence-specific guideline is available. Available at https://www.sentencingcouncil.org.uk/overarching-guides/crown-court/item/general-guideline-overarching-principles/.

3 Sentencing Council Definitive Guideline, Corporate offenders: fraud, bribery and money laundering, effective from 1 October 2014, available at https://www.sentencingcouncil.org.uk/offences/crown-court/item/corporate-offenders-fraud-bribery-and-money-laundering/.

4 Coroners and Justice Act 2009, s.125(1).

© Law Business Research 2021

offence[5] (although the court cannot exceed the maximum sentence available at the time of the commission of the offence) to ensure that the sentence passed is in the interests of justice.

The sentencing guidelines set out a step-by-step process for sentencing offenders. The Guideline contains 10 steps:

- compensation;
- confiscation;
- determining the offence category;
- starting point and category range;
- adjustment of fine;
- factors that would indicate an adjustment;
- reduction for guilty pleas;
- ancillary orders;
- totality principle;
- reasons.

The steps are explained in further detail below.

Compensation 25.2

The court must first consider ordering a company to pay compensation to a victim of offending for any personal injury, loss or damage resulting from the offence,[6] in an amount it considers appropriate. The court will have regard to any evidence and any representations made by the prosecutor or the company[7] and must consider the company's ability to pay.[8] If a company does not have the means to pay both a fine and a compensation order, a compensation order will take priority.[9] Compensation orders are not mandatory, but if the court does not make one it must give reasons for the decision.[10]

Confiscation 25.3

The second step under the Guideline is for the court to consider confiscation. The confiscation regime is governed by the Proceeds of Crime Act 2002. The court must consider confiscation where the prosecutor asks it to proceed or where the court considers it appropriate to do so,[11] and confiscation must be dealt with before any other fine or financial order (except compensation).[12] The purpose of a confiscation order is to recover a sum of money equal to the benefit obtained from the offence, whether or not it has been retained.

5 *R v. H & Ors* [2011] EWCA Crim 2753; *R v. Clifford* [2014] EWCA Crim 2245.

6 Powers of Criminal Courts (Sentencing) Act 2000, s.130(1).

7 ibid., s.130(4).

8 ibid., s.130 (11).

9 ibid., s.130(12).

10 ibid., s.130(3).

11 Proceeds of Crime Act 2002, s.6.

12 ibid., s.13.

© Law Business Research 2021

The court will consider (1) whether the defendant has benefited from criminal conduct, (2) the value of the benefit obtained and (3) what sum is recoverable from the defendant.

The defendant's criminal benefit is the value of the property obtained as a result of, or in connection with, the criminal conduct, including any pecuniary advantage.[13]

In calculating the benefit, the court must first consider whether the defendant has a 'criminal lifestyle'.[14] Circumstances where a criminal lifestyle will be found include where a defendant is convicted of money laundering offences;[15] where the defendant has obtained benefit of at least £5,000, where the offence forms part of a course of criminal activity;[16] or where it is committed over six months or more.[17] Given that serious economic offences are often committed over lengthy periods, (especially where charged as a conspiracy), the criminal-lifestyle provisions are often engaged. Where a criminal lifestyle is found, the court will decide whether the defendant has benefited from 'general criminal conduct'[18] namely, any of his or her criminal conduct, whenever it occurred and regardless of whether there it has ever been prosecuted.[19] When calculating the benefit to a defendant with a 'criminal lifestyle', the court may draw certain assumptions about the defendant's property,[20] which can be very detrimental to a defendant. For example, it may assume that any property transferred to the defendant in the six years preceding a charge was obtained by criminal conduct. However, the defendant may prove that an assumption is incorrect, and the court may not draw an assumption where it would give rise to a serious risk of injustice.[21]

If the defendant is not considered to have a criminal lifestyle, the court must consider whether the defendant has benefited from the criminal conduct[22] for which he or she is being sentenced and determine the value of that benefit. The court must then decide the recoverable amount and make a confiscation order requiring the defendant to pay,[23] unless the defendant can show the available amount is less than the benefit, in which case the recoverable amount will be the available amount, or a nominal amount, if nothing is available.[24] The

13 ibid., s.76(4) and (5).

14 ibid., s.6(4)(a). 'Criminal lifestyle' is defined in s.75 Proceeds of Crime Act 2002.

15 ibid., s.75(2)(a). The section provides for specified lifestyle offences that are set out in Schedule 2 of the Act.

16 ibid., s.75(2)(b).

17 ibid., s.75(2)(c).

18 ibid., s.6(4)(b).

19 ibid., s.76(2).

20 ibid., s.10.

21 ibid., s.10 (6)(a) and (b).

22 ibid., s.6(4)(c).

23 ibid., s.6(5).

24 ibid., s.7(2).

© Law Business Research 2021

available amount is the aggregate of the value of the defendant's free property and any tainted gifts made by the defendant, less the value of any obligations that take priority.[25]

A confiscation order is an order to pay a sum of money, but it can be enforced against the defendant's property and any tainted gifts, if the defendant fails to pay.

Before making an order, the court must consider whether a confiscation order is proportionate.[26] Case law suggests that it is not proportionate to take the entire value of a corrupt contract as the benefit (where full value is given under the contract), but rather that proportionality dictates that the benefit should be confined to the gross profit, together with any other pecuniary advantage flowing from the corruption.[27] The amount of any bribes paid will be added back if they have been deducted as an expense when reaching the gross profit. In a separate case, it has been held that where the defendant can establish that VAT output tax on revenue obtained from criminal conduct has been paid to HM Revenue and Customs, it would be disproportionate to make a confiscation order calculated on the basis that a sum equivalent to that VAT paid has been 'obtained' by the defendant.[28]

Fine 25.4

In determining the level of fine, the Guideline requires the court to first assess the offence category, by reference to the company's culpability and the harm caused. The Guideline sets out three categories of culpability – high, medium and lesser; and provides a non-exhaustive list of characteristics that may demonstrate each level. The court should weigh up all the factors of the case to determine the company's culpability.

The harm figure is a financial sum that represents the amount obtained or loss avoided (or intended to be obtained or avoided). For fraud offences and cheating the revenue, the harm is generally the actual or intended gross gain to the company. For offences under the Bribery Act[29] the harm figure will generally be the gross profit from the contract obtained, retained or sought as a result of the offending. Where the offence is failing to prevent bribery,[30] the likely cost avoided by the company in failing to put adequate procedures in place may be used as an alternative measure. For money laundering offences, the harm figure will generally be the amount laundered or the likely cost avoided by failing to put in place an effective anti-money laundering programme (if this is higher). If the actual or intended gain cannot be established, the harm figure will be the amount that the court considers was likely to be achieved in

25 ibid., s.9.

26 *R v. Waya* [2012] 3WLR 1138; Proceeds of Crime Act 2002, s.6(5).

27 *R v. Sale* [2013] EWCA Crim 1306.

28 *R v. Harvey* [2016] 4 All ER 521.

29 UK Bribery Act 2010.

30 ibid., s.7.

© Law Business Research 2021

all the circumstances. The Guideline also suggests that in large cases in which the true harm is to commerce or markets generally, a harm figure in excess of those guidelines may be justified.

A multiplier is then applied to the harm figure according to the category of culpability. The Guideline sets out a table with the starting point and range for each culpability level. For high culpability, the starting point is a multiplier of 300 per cent; for medium culpability, 200 per cent; and for lesser culpability, 100 per cent. Once the court has determined the appropriate starting point, it must consider adjustment within the range provided for aggravating and mitigating factors (although the Guideline also suggests that in some cases it may be appropriate to use a figure outside the category range). A non-exhaustive list of such factors is set out in the Guideline.

The fine must reflect the seriousness of the offence and take into account the financial circumstances of the offender.[31]

Once the court has arrived at the fine, it is required to 'step back' and consider the overall effect. The combination of compensation, confiscation and fine is supposed to (1) remove all gain, (2) punish appropriately and (3) deter. The court should consider whether there are any further factors that may require an adjustment and ensure those aims are met fairly. Examples set out in the Guideline include the impact of any fine on the company's ability to implement an effective compliance programme, or on the employment of staff or on the local economy.

If a company is being sentenced for more than one offence, the court should also apply the 'totality principle': it should consider whether the total sentence is just and proportionate to the offending.[32]

A defendant may seek an indication in advance of the maximum sentence that would be imposed were he or she to plead guilty at that stage of proceedings, although a judge may also refuse to give one. This is known as a '*Goodyear* indication'[33] and is binding on the court once given; although if the defendant chooses not to plead guilty at that stage, it ceases to be binding.

25.5 Guilty plea

Where a defendant pleads guilty, the court must consider a reduction in sentence,[34] having regard to the 'Reduction in Sentence for a Guilty Plea Guideline' (the Plea Guideline).[35] The level of reduction is determined by the stage at which the defendant pleads guilty and the circumstances in which it

31 Criminal Justice Act 2003, s.164.

32 Step 9 of the Guideline. There is also an overarching 'Totality Guideline', available at https://www.sentencingcouncil.org.uk/overarching-guides/crown-court/item/totality/.

33 *R v. Goodyear* [2005] EWCA Crim 888; Criminal Practice Direction, VII Sentencing, C, Indications of sentence: *R v. Goodyear*.

34 Criminal Justice Act 2003, s.144; Step 7 of the Guideline.

35 Sentencing Council, 'Reduction in sentence for a guilty plea – first hearing on or after 1 June 2017', effective from 1 June 2017, available at https://www.sentencingcouncil.org.uk/

© Law Business Research 2021

was given, but it cannot exceed one third of the sentence. A defendant will generally receive a discount of one third if a guilty plea is entered at the first stage of proceedings, which is generally the first hearing at which a plea or indication of plea is sought and recorded by the court.[36]

For a guilty plea entered after the first stage, the maximum discount available is one quarter up until the first day of trial, when a maximum of one-tenth is available. For pleas entered subsequently during the trial, the discount will reduce again, potentially to zero. The Plea Guideline sets out exceptions where the discounts may not be applied as described, for example, for certain offences that have minimum or appropriate sentences prescribed by statute.

The court should also consider any other factors that would justify a reduction, such as co-operation by the defendant with the investigation or prosecution.[37]

Costs 25.6

The court may make a costs order in favour of either the prosecution or the defendant.[38] Ordinarily, in the event of a conviction, the defendant will be ordered to pay costs to the prosecutor that the court considers just and reasonable.[39] If a defendant is acquitted or the prosecution does not proceed to trial, the court may make an order in favour of the defendant of an amount the court considers reasonably sufficient to compensate for any expenses properly incurred in the proceedings.[40]

overarching-guides/crown-court/item/reduction-in-sentence-for-a-guilty-plea-first-hearing-on-or-after-1-june-2017/.

36 A one-third discount may still be given after that stage if the court is satisfied that circumstances significantly reduced the defendant's ability to understand what was alleged or otherwise made it unreasonable to expect the defendant to indicate a guilty plea sooner. However, a distinction is made between cases where a defendant needs to receive advice or see evidence to understand whether he or she is in fact guilty of the offence (in which case the defendant may still receive a one-third discount), and cases where the defendant merely delays entering a plea to assess the strength of the prosecution evidence and the prospects of being convicted or acquitted (where the defendant will not receive a discount).

37 Serious Organised Crime and Police Act 2005, ss.73 and 74; Step 6 of the Guideline.

38 Criminal Practice Directions 2015 [2015] EWCA 1567; Practice Direction (Costs in Criminal Proceedings) 2015 [2015] EWCA Crim 1568; Prosecution of Offences Act 1985, Part II (ss.16 to 19B); Access to Justice Act 1999; Legal Aid, Sentencing and Punishment of Offenders Act 2012 (in relation to funded clients); Costs in Criminal Cases (General) Regulations 1986.

39 Prosecution of Offences Act 1985, s.17.

40 ibid., s.16.

© Law Business Research 2021

25.7 Director disqualifications

Under the Company Directors Disqualification Act 1986 (CDDA), any director convicted of misconduct[41] in connection with a company (either in the United Kingdom or overseas) or considered unfit to be concerned with the management of a company, may be disqualified from the right to manage a company for up to 15 years by a disqualification order.[42] The person will also be entered on the register of disqualified directors. The definition of 'director' is very wide, and has been interpreted to include former directors, shadow directors and senior managers who may be considered to be acting as directors of the company.[43]

Where there is a conviction in respect of an indictable offence,[44] usually the sentencing court will consider whether a disqualification order ought to be made and impose it. However, the Insolvency Service[45] may also look to bring separate disqualification proceedings, before or even alongside, a criminal prosecution irrespective of whether the company in question is solvent.

The Secretary of State also may apply to court for a disqualification order if it appears expedient in the public interest, and the court may grant it where it is satisfied that a person's conduct in relation to the company (alone or taken together with his or her conduct as a director of other companies or overseas companies) makes that person unfit to be concerned in the management of a company.[46] For offences committed outside the United Kingdom, the Secretary of State may apply to the court for a disqualification order.[47]

25.8 Civil recovery orders

Some enforcement agencies[48] may obtain a civil recovery order (CRO) to recover proceeds of crime where it is proved, on the balance of probabilities,

41 Sections 2 to 5A of the Company Directors Disqualification Act 1986 set out the misconduct for which a director can be disqualified.

42 Company Directors Disqualification Act 1986, ss.2(1), 5A(2) and 8(2).

43 Companies Act 2006, s.250; see *Revenue and Customs Commissioners v. Holland* [2010] UKSC 51 for consideration of the definition in practice. In this case, the Supreme Court confirmed there is no definitive test for when a person may be considered a *de facto* director, and the question should be whether they have assumed responsibility to act as a director in relation to the company in question.

44 In addition, any conviction in connection with the liquidation or striking off of a company, with the receivership of a company's property or with being an administrative receiver of a company's property may also result in a disqualification order: section 21, Company Directors Disqualification Act 1986.

45 See https://www.gov.uk/government/organisations/insolvency-service.

46 Company Directors Disqualification Act 1986, s.8.

47 ibid., s.5A.

48 The Serious Fraud Office (SFO), the National Crime Agency (NCA), the Crown Prosecution Service (CPS), HM Revenue and Customs and the Financial Conduct Authority (FCA) may obtain such orders.

© Law Business Research 2021

that the property has been obtained unlawfully.[49] Such property is 'recoverable property' and it is vested in a trustee appointed to realise the property to maximise the amount payable to the enforcement agency.[50]

A CRO is made in respect of specific property, and no conviction is required. Recent guidance issued in 2021 by the Home Office in relation to the use of asset recovery powers by relevant enforcement agencies[51] states that non-conviction based asset recovery powers may be sought whether or not there is a criminal investigation or prosecution and regardless of what stage any criminal investigation or prosecution may have reached.

In 2018, the Serious Fraud Office (SFO) obtained a significant CRO in respect of Griffiths Energy, a company that had pleaded guilty to bribery charges in Canada relating to bribing Chadian diplomats in the United States and Canada to secure contracts. The SFO recovered £4.4 million of the proceeds of the crime that had been traced to a bank account in London.[52] The recovered funds were to be transferred to the Department for International Development who were to identify key projects to invest in to benefit the people of Chad.[53]

The High Court also may make unexplained wealth orders.[54] These require politically exposed persons or persons suspected of involvement in serious crime to explain how they obtained assets that appear to be disproportionate to their known income. A failure to provide a response will give rise to a presumption that the property is recoverable in civil recovery proceedings.

Certain enforcement agencies may seize and detain cash or listed assets[55] of £1,000 or more where they have reasonable grounds to suspect that it is recoverable property or intended for use in unlawful conduct.[56] A magistrate may extend the period of detention.[57] An application can be made to the court for an account freezing order in relation to money in bank accounts on the same grounds.[58] Cash, and money in frozen bank accounts, will be automatically forfeited if no objection is raised to a forfeiture notice.[59] The magistrates' court

49 Pursuant to Part 5, Proceeds of Crime Act 2002.

50 Proceeds of Crime Act 2002, ss. 266(2) and 267.

51 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1001245/June_2021_amended_s.2A_guidance_.pdf.

52 *SFO v. Saleh* [2018] EWHC 1012 (QB). For another example of significant civil recovery order against a corporate, see the 2012 CRO against Oxford Publishing Limited, at https://www.sfo.gov.uk/2012/07/03/oxford-publishing-ltd-pay-almost-1-9-million-settlement-admitting-unlawful-conduct-east-african-operations/.

53 https://www.sfo.gov.uk/2018/03/22/sfo-recovers-4-4m-from-corrupt-diplomats-in-chad-oil-share-deal/.

54 Criminal Finances Act 2017, ss.1 to 9. Applications can be made by the SFO, NCA and FCA, among others.

55 Proceeds of Crime Act 2002, s.303B.

56 ibid., ss.294, 295, 303J and 303K.

57 ibid., ss.295(2) and 303L.

58 ibid., ss.303Z1 to 303Z3.

59 ibid., ss.297A-297E and 303Z9-303Z13.

© Law Business Research 2021

may order forfeiture of cash, listed assets or money in frozen bank accounts where it is satisfied the assets are recoverable property or intended for use in unlawful conduct.[60]

The NCA may also tax the proceeds of crime where they represent income in respect of which tax has not been paid.[61]

25.9 Criminal restraint orders

Restraint orders can be made to freeze assets at any time following the commencement of a criminal investigation up until the conclusion of proceedings.[62] An order will be granted at the investigation stage if there are reasonable grounds to suspect that an alleged offender has benefited from his or her criminal conduct;[63] or, if proceedings have begun, if there is reasonable cause to believe the defendant has benefited from his or her criminal conduct.[64] An order should only be made where there is a real (rather than fanciful) risk that assets will be dissipated if an order is not made.[65] If necessary, an allowance will be made from the restrained property for the defendant's reasonable living expenses[66] and to enable a person to carry on any trade, business, profession or occupation.[67] Provision may also be made for reasonable legal expenses, but not if they are incurred in connection with the offences in respect of which the restraint order has been made.[68]

25.10 Serious crime prevention orders

Serious crime prevention orders (SCPOs)[69] are injunctions[70] that can be imposed on a person been convicted of a serious offence[71] or who has 'been

60 ibid., ss.298, 303O and 303Z14.

61 ibid., Part 6.

62 ibid., s.40.

63 ibid., s.40(2)(b).

64 ibid., s.40(3)(b).

65 *Re AJ & DJ* (Unreported), 9 December 1992, CA.

66 Proceeds of Crime Act 2002, s.41(3)(a).

67 ibid., s.41(3)(b).

68 ibid., ss.41(3)(a) and 41(4).

69 SCPOs were introduced in the Serious Crime Act 2007 and significantly broadened by the Serious Crime Act 2015.

70 Serious Crime Act 2015, s.35(1).

71 The Crown Court has jurisdiction to make an SCPO where a person has been convicted of a 'serious offence' in the Crown Court or in the magistrates' court where they committed to the High Court for sentence; s.19(1), paras. (a) and (b) Serious Crime Act 2007. A 'serious offence' is defined in s.2(2), paras. (a) and (b) Serious Crime Act 2007 as an offence that is specified In Part 1 of Schedule 1 to the Act, or an offence the court considers to be sufficiently serious to be treated as if it were so specified.

© Law Business Research 2021

involved in serious crime'[72] where there are reasonable grounds to believe that making an SCPO would protect the public by preventing, restricting or disrupting involvement by the person in serious crime in England and Wales. The court may include such terms in an SCPO as it considers appropriate for the purpose of so protecting the public;[73] but they must be proportionate to the identified risk. Restrictions that might be imposed include limitations on financial, property or business dealings;[74] a person's associations or communications;[75] use of any item;[76] and travel both within and outside the jurisdiction.[77] An SCPO may also include a requirement to provide specified information or disclose documents to law enforcement.[78]

Breach of an SCPO is a criminal offence. The maximum sentence for an individual five years' imprisonment.[79] Where a corporation is convicted of a breach of an SCPO, the court may order its dissolution where to do so would be 'just and equitable'.[80]

Regulatory financial penalties and other remedies 25.11

Companies and individuals may also face regulatory sanctions for their misconduct separately or in addition to criminal penalties.

The Financial Conduct Authority (FCA) regulates firms and individuals performing regulated financial services activities and may bring enforcement action against regulated firms and individuals in connection with economic

72 The High Court has jurisdiction to make an SCPO where a person has 'been involved in serious crime'; Serious Crime Act 2007, s.1, paras. (a) and (b). Such a finding can be made in the absence of a conviction. Persons have been involved in serious crime if they have (1) committed a serious offence, (2) facilitated the commission by another person of a serious offence, or (3) conducted themselves in a way that was likely to facilitate the commission by themselves or another person of a serious offence, whether or not such an offence was committed; ibid., s.2(1), paras. (a) to (c).

73 Serious Crime Act 2015 (High Court), s.1(3); s.19(5) (Crown Court). Other legislation dealing with civil orders in furtherance of the criminal law, such as anti-social behaviour orders, sexual offences prevention orders, and terrorism prevention and investigation measures impose a requirement of 'necessity' rather than 'appropriateness'. As most applications for an SCPO will engage one or more rights under the European Convention on Human Rights, however, the court will need to consider the Human Rights Act 1998, in particular the precept of proportionality, which includes necessity. See also CPS guidance on serious crime prevention orders (Terms of orders), available at https://www.cps.gov.uk/legal-guidance/serious-crime-prevention-orders.

74 Serious Crime Act 2015, s.5(3)(a).

75 ibid., s.5(3)(c).

76 ibid., s.5(3)(e).

77 ibid., s.5(3)(f).

78 ibid., s.5(5)(a). But a requirement to provide information orally is not permissible: ibid., s.11.

79 Serious Crime Act 2003, s.25.

80 ibid., s.27.

© Law Business Research 2021

crimes if it considers there has been a regulatory breach.[81] It may also take action against persons who carry out regulated activities without FCA authorisation. The FCA's Enforcement Guide (EG) describes the FCA's approach to exercising its enforcement powers, and Chapter 7 summarises its powers to impose financial penalties and other sanctions.

The FCA's Decision Procedure and Penalties Manual (DEPP) sets out its policy for the imposition and amount of financial penalties (among other things).

The regime for setting financial penalties is based on three principles: (1) disgorgement, (2) discipline and (3) deterrence.[82]

The total amount payable will comprise disgorgement of any benefit received and a financial penalty reflecting the seriousness of the breach.[83] These elements are incorporated in a five-step process to determine the level of a financial penalty to be imposed on a firm for a regulatory breach, as follows:[84]

1 Removal of any financial benefit derived from the breach (which may include the profit made or loss avoided), plus interest. Where a firm's entire business model depends on breaching FCA rules or other regulatory requirements and the breach is at the core of the firm's regulated activities, the FCA will seek to deprive the firm of all the financial benefit derived from such activities.[85]
2 Determining a figure reflecting the seriousness of the breach.[86] In many cases the FCA considers the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause. In those cases, the FCA will determine the firm's revenue from the relevant products or business areas during the breach, called the 'relevant revenue'. The figure will be a percentage of this from 0 per cent to 20 per cent, applied on a sliding scale to reflect the seriousness of the breach, taking into account factors set out in DEPP 6.5.2A.
3 Mitigating and aggravating factors[87] are applied to increase or decrease the figure reached at step 2.
4 If the FCA considers the figure arrived at after step 3 is an insufficient deterrent, it may increase the penalty.[88]
5 A settlement discount is applied, if appropriate, to reflect the stage at which the FCA and the firm reached agreement.[89]

81 The FCA may also institute proceedings for certain criminal offences, for example insider trading, under Financial Services and Markets Act (FSMA) 2000, ss.401 and 402.

82 DEPP 6.5.2.

83 ibid., 6.5.3(1).

84 ibid., 6.5A.

85 ibid., 6.5A(1).

86 ibid., 6.5A(2).

87 ibid., 6.5.A(3).

88 ibid., 6.5A(4) provides examples of circumstances when this may occur.

89 ibid., 6.5A (5).

© Law Business Research 2021

The FCA introduced a new enforcement procedure for disciplinary cases in 2017, under which four settlement options are available for resolving matters at an early stage in proceedings. These are:

- 30 per cent discount if the party settles the factual issues, the fact of a regulatory breach and the amount of penalty with the FCA;
- 30 per cent discount if the party agrees with the FCA all the relevant facts and accepts that they amount to regulatory breaches, whether or not it disputes the penalty to be imposed;
- 15 to 30 per cent discount if the party agrees with the FCA all the relevant facts but disputes that they amount to regulatory breaches and disputes the penalty; or
- 0 to 30 per cent discount if the party reaches partial agreement with the FCA as to facts, liability and penalty but disputes a narrow set of issues.[90]

This gives regulated firms the ability to receive discounts where they accept some aspects of the case but to keep their right to challenge certain aspects of the FCA's findings before the Regulatory Decision Committee.[91]

In 2020, the FCA levied fines that totalled just over £192.5 million.[92]

Withdrawing a firm's authorisation 25.12

In addition to imposing financial penalties on authorised firms and individuals, the FCA has a number of other powers including powers to issue public censures and to withdraw authorisation to engage in regulated activities. A common form of authorisation is permission given by the FCA to a firm under Part 4A of the Financial Services and Markets Act (FSMA) 2000 to carry on regulated activities. The FCA's powers include a right to cancel this permission if it appears to the FCA that the authorised person is failing or is likely to fail to fulfil the threshold conditions.[93] Withdrawal of permission means that the person ceases to be authorised and cannot engage in regulated activities.[94] As an alternative to withdrawing permission, the FCA has broad powers to vary a Part 4A permission or to impose specific conditions on its exercise instead.[95] The EG states that the cancellation power will be exercised mainly where the FCA has 'very serious concerns'[96] about a firm, or the way its business is or has been conducted, and sets out a list of non-exhaustive examples of circumstances

90 FCA Enforcement Information Guide, April 2017, p. 4, available at https://www.fca.org.uk/publication/corporate/enforcement-information-guide.pdf.

91 https://www.fca.org.uk/publication/corporate/enforcement-information-guide.pdf.

92 https://www.fca.org.uk/news/news-stories/2020-fines.

93 FSMA 2000, s.55J(1)(a). The FCA may also cancel permission if the authorised person has not engaged in regulated activity in the previous 12 months: ibid., s.55J(1)(b).

94 ibid., ss.19 and 31(1)(a).

95 ibid., ss.55J and 55L.

96 FCA's Enforcement Guide (EG) 8.5.1.

© Law Business Research 2021

in which the FCA may cancel a firm's permission.[97] These include, for example, where there are repeated failures to comply with rules or requirements,[98] or where there has been a failure to co-operate with the FCA of sufficient seriousness that the FCA ceases to be satisfied that the firm is fit and proper.[99]

25.13 Approved persons

The Approved Persons Regime regulates individuals exercising certain functions on behalf of regulated entities. Approved persons are approved by the FCA to exercise 'controlled functions' at an authorised firm. They must know and meet the relevant regulatory requirements, meet the fitness and propriety test, and comply with the FCA Conduct Rules.[100] They have a duty to report to the FCA anything that could affect their ongoing suitability to be an approved person. Senior management functions are a subset of controlled functions. A person holding a designated senior management function has an additional 'duty of responsibility' so that if a firm breaches a regulatory requirement, the senior manager responsible for managing the relevant area will also be held accountable for the breach if they did not take 'such steps as a person in their position could reasonably be expected to take' to avoid the breach occurring or continuing.[101]

Where approved persons (including senior managers) have committed a regulatory breach, they may receive a financial penalty or a public censure.[102] They may also have their approval withdrawn or be prohibited from performing functions in relation to regulated activities,[103] or both. The FCA may also issue private warnings.

25.14 Restitution orders

The FCA may seek restitution where it seeks to compensate those adversely affected by a regulatory breach.

The FCA will take the following considerations into account in determining whether to seek restitution, in the light of 'all the circumstances of the case':

- whether the profits are quantifiable or the losses identifiable;
- the number of persons affected;
- costs to the FCA of securing restitution;
- availability of alternative redress, such as compensation schemes or through another regulator;
- whether victims can be expected to bring proceedings in their own right;
- the firm's solvency;

97 EG 8.5.2

98 ibid., 8.5.2(7).

99 ibid., 8.5.2(8)

100 FCA Handbook Code of Conduct (COCON).

101 FSMA 2000, s.66A(5).

102 ibid., s.66.

103 ibid., s.56.

© Law Business Research 2021

- alternative powers available to the FCA; and
- the conduct of persons having suffered loss, for example whether they have contributed to their loss.[104]

This list is not exhaustive. The FCA can apply for restitution to a court, which may order payment of a sum it considers 'just' having regard to the profits made or loss caused.[105]

Where appropriate, the FCA will consider imposing a restitution order using its administrative powers[106] where the FCA is 'satisfied that a person has contravened a relevant requirement, or been knowingly concerned in the contravention of such a requirement'.[107] The person against whom the order is sought must either have profited from the contravention, or caused loss or other adverse effect to another.[108]

Debarment 25.15

Companies need to be mindful of the impact that any conviction, or even misconduct not resulting in a conviction, may have on their ability to tender for public contracts. The rules governing debarment are contained in the Public Contracts Regulations 2015 (the Regulations).[109]

Debarment can be mandatory or discretionary. Debarment is mandatory if the tendering company has been convicted of certain offences, including:

- bribery;[110]
- corruption; and
- money laundering.[111]

A company may also face mandatory debarment if certain individual representatives of the company are convicted of one or more of these offences.[112] Mandatory debarment applies for a maximum of five years.

104 EG 11.2.1.

105 FSMA 2000, s.382(2).

106 ibid., s.384.

107 ibid., s.382(1) and (6). The meaning of 'relevant requirement' is somewhat narrower than under the injunction provisions, but is substantially the same: see ibid., s.382(9).

108 ibid., s.382(2).

109 These came into force on 26 February 2015 and implemented the EU Procurement Directive (Directive 2014/24/EU) in the United Kingdom.

110 Specifically, the common law offence of bribery; corruption within the meaning of s.1(2) Public Bodies Corrupt Practices Act 1889; corruption within the meaning of s.1 Prevention of Corruption Act 1906; bribery within the meaning of s.1, s.2 or s.6 Bribery Act 2010; or bribery within the meaning of s.113 Representation of the People Act 1983. The failure of a commercial organisation to prevent bribery, contrary to s.7 Bribery Act 2010, will not trigger mandatory debarment but may result in discretionary debarment.

111 Public Contracts Regulations 2015, Regulation 57.

112 ibid., Regulation 57(1).

© Law Business Research 2021

The Regulations set out a list of circumstances in which discretionary debarment may apply.[113] One of these is where a contracting authority is able to demonstrate, by appropriate means, that a company is guilty of grave professional misconduct rendering its integrity questionable. Discretionary debarment applies for a maximum of three years.[114]

In 2015, the United Kingdom adopted the European Union's concept of 'self-cleaning' in relation to mandatory and discretionary debarment. The Regulations set out a number of conditions that, if met, can demonstrate a company's suitability for access to public procurement tenders despite the existence of grounds for mandatory or discretionary debarment. The conditions include the payment of compensation, co-operation with investigative authorities and the taking of concrete measures to prevent further criminal offences or misconduct being committed.[115]

25.16 Outcomes under a DPA

The legislation, the SFO's Operational Handbook[116] and DPA Code of Practice[117] state that the level of financial penalty imposed in a DPA should be comparable to a fine that a court would have imposed following a guilty plea.[118] The DPA Code states that this approach is intended to enable the parties and courts to have regard to relevant sentencing principles and guidelines to determine the appropriate level for a financial penalty. The Director of the SFO has stated that, since DPAs were introduced, they have delivered penalties, costs and returned illicit gains worth more than £1.5 billion.[119]

In all but two DPAs[120] approved by the court, a discount of around 50 per cent of the financial penalty has been applied. This figure has been reached by taking an initial one-third discount, equivalent to a guilty plea at the earliest stage, and adding a further discount on the basis of co-operation

113 ibid., Regulation 57(8).

114 ibid., Regulation 57(12).

115 ibid., Regulation 57(15).

116 The SFO's Operational Handbook was updated to include a chapter on DPAs in October 2020, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/deferred-prosecution-agreements/.

117 Crime and Courts Act 2013; SFO and CPS, Deferred Prosecution Agreements Code of Practice, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/.

118 Crime and Courts Act 2013, Schedule 17, para. 5(4); DPA Code, para. 8.3.

119 Lisa Osofsky, 'We're defending the UK as a safe place for business', *The Times* (London, 30 June 2021).

120 *SFO v. Standard Bank Plc (Now known as ICBC Standard Bank Plc)* [2016] Lloyd's Rep FC Plus 122; *SFO v. G4S Care and Justice Services (UK) Limited*, [2020] 7 WLUK 303, para. 40. Standard Bank only received a one-third reduction in penalty for promptly reporting its own conduct and co-operating with the SFO's subsequent investigation. This was considered a 'full reduction' in this matter. G4S received a 40 per cent reduction in penalty.

© Law Business Research 2021

and remediation activities. This discount is likely to be consistent with what would be imposed under the Guideline, which directs reductions for guilty pleas and co-operation.

For example, in the *Sarclad Limited* DPA, Sir Brian Leveson, then President of the Queen's Bench Division, considered that a 50 per cent reduction was appropriate as the company had self-reported in a timely way and had fully co-operated with the SFO.[121] A similar justification also prompted 50 per cent discounts for the *Tesco*, *Serco Geografix, Airline Services* and *Amec Foster Wheeler* DPAs.[122]

Even where companies have not self-reported, some have still received 50 per cent reductions in financial penalty when they have provided extensive co-operation after the investigation began. Rolls-Royce did not self-report to the SFO. Although Airbus technically did self-report, it had known of concerns for some time and reported only once it was notified that UKEF considered it was obliged to disclose the matter to the SFO.[123] The court, in approving the DPA, stated: 'Airbus could have moved more quickly.'[124] However, both received a 50 per cent reduction in penalty owing to 'extraordinary co-operation' on the part of Rolls-Royce and 'exemplary co-operation and remediation' by Airbus.[125] By contrast, G4S self-reported but only received a 40 per cent reduction in penalty. Its co-operation fell short of being exemplary or extraordinary, and full co-operation was said to have come 'relatively late in the day'. However, a discount of more than one-third was considered appropriate because of the overall level of co-operation and the unusually wide scope of the self-cleaning steps taken by G4S.[126]

In the *Güralp* DPA (where Güralp self-reported), the SFO sought to impose no financial penalty. This was on the basis that to do so would cause the organisation to become insolvent, disproportionately impacting the business, and would also cause harm to the organisation's innocent employees.[127]

The mandatory debarment provisions of the Public Contracts Regulations 2015 will not apply because the entry into a DPA does not constitute a conviction. However, a company may still be at risk of discretionary debarment if the conduct underlying the DPA is considered 'grave professional misconduct', in accordance with the Regulations.

---

121 *SFO v. Sarclad Limited* [2016] Lloyd's Rep FC 509, para. 69.

122 *SFO v. Tesco Ltd* [2017] 4 WLUK 558; *SFO v. Serco Geografix Ltd* [2019] 7 WLUK 45; *SFO v. Airline Services Limited* Case No. U20201913.

123 *SFO v. Airbus SE* [2020]: Statement of Facts prepared pursuant to Schedule 17, para. 5(1) Crime and Courts Act 2013, paras. 33 and 34, available at https://www.sfo.gov.uk/download/airbus-se-deferred-prosecution-agreement-statement-of-facts/

124 *SFO v. Airbus SE* [2020] 1 WLUK 435, para. 73.

125 *SFO v. Airbus SE* [2020] 1 WLUK 435, para. 112; *SFO v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc*, [2017] Lloyd's Rep FC 249, para. 123.

126 *SFO v. G4S Care and Justice Services (UK) Limited,* [2020] 7 WLUK 303, para. 40.

127 *SFO v. Güralp Limited* [2019] Case No. U20190840, para. 35.

© Law Business Research 2021

26

Fines, Disgorgement, Injunctions, Debarment: The US Perspective

Anthony S Barkow, Charles D Riely, Amanda L Azarian and Grace C Signorelli-Cassady[1]

26.1 Introduction

This chapter provides an overview of the potential fines, penalties and other collateral consequences that corporates and individuals may face in the United States under federal law when defending against, or settling an enforcement action with, US authorities. The chapter then provides examples of the fines, penalties and other remedies associated with particular federal criminal statutes of potential interest, including the Foreign Corrupt Practices Act and anti-money laundering statutes.

US enforcement authorities have a variety of means to seek redress from corporates and individuals, including financial penalties and equitable remedies. The general purpose and policy objectives behind these remedies are (1) to deter the defendant and others from committing such offences in the future, (2) to protect the public, (3) to punish the defendant and (4) to promote rehabilitation of the defendant.[2] In considering fines and penalties, the US enforcement authorities and courts will consider the facts and circumstances of the matter, including whether the defendant accepts responsibility for the conduct, any remediation that has been effected and co-operation by the defendant with the relevant enforcement authorities.[3]

See Chapter 10 on co-operating with authorities

1 Anthony S Barkow and Charles D Riely are partners, and Amanda L Azarian and Grace C Signorelli-Cassady are associates, at Jenner & Block LLP. The authors wish to acknowledge the contribution of Rita D Mitchell of Willkie Farr & Gallagher, the original author of the chapter in previous editions on which this chapter is partly based.

2 See, e.g., Department of Justice (DOJ), Justice Manual (Justice Manual) § 9-27.110.

3 See, e.g., Justice Manual § 9-27.420.

© Law Business Research 2021

In recent years, both the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) have been successful in extracting significant financial penalties as part of their enforcement actions and settlements. These penalties depend on the facts and circumstances and range from penalties in the five- to six-figure range[4] to settlements in the billions.[5] These include cases brought by the DOJ, individual US attorney offices and the SEC. For example, in the fiscal year ending in September 2020, the DOJ obtained more than US$2.2 billion in total settlements and judgments from civil cases brought pursuant to the False Claims Act alone.[6] Likewise, in 2020, the US Attorney's Office for the Eastern District of Virginia, which includes some of the area surrounding Washington, DC, collected more than US$242 million in criminal and civil actions.[7] The Southern District of New York announced two settlements in 2020, totalling nearly US$90 million between them alone.[8] In fiscal year 2020, the SEC brought 715 enforcement actions and obtained

4 See, e.g., DOJ press release, 'Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations' (31 May 2019), available at https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations; Department of Justice press release, 'Department Of Justice Reaches $5.5 Million Settlement With Van Andel Research Institute To Resolve Allegations Of Undisclosed Chinese Grants To Two Researchers' (19 Dec. 2019), available at https://www.justice.gov/usao-wdmi/pr/.

5 For example, in October 2020, the DOJ and SEC entered into the largest FCPA settlement to date with Goldman Sachs Group and its Malaysian subsidiary. The agencies imposed financial penalties totalling approximately US$3.3 billion to resolve charges in connection with a large-scale bribery scheme. (DOJ press release, 'Goldman Sachs Charged in Foreign Bribery Case and Agrees to Pay Over $2.9 Billion' (22 Oct. 2020), available at https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion). Also in 2020, the SEC obtained a US$500 million penalty against Wells Fargo for misleading investors by opening 'authorized or fraudulent accounts for unknowing customers' (Securities and Exchange Commission, Division of Enforcement 2020 Annual Report, available at https://www.sec.gov/files/enforcement-annual-report-2020.pdf.).

6 DOJ press release, 'Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020' (14 Jan. 2021), available at https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020.

7 DOJ press release, 'U.S. Attorney's Office in EDVA Recovers $242 Million in 2020 for Victims and in Criminal and Civil Matters' (8 Feb. 2021), available at https://www.justice.gov/usao-edva/pr/us-attorney-s-office-edva-recovers-242-million-2020-victims-and-criminal-and-civil.

8 DOJ press release, 'Acting Manhattan U.S. Attorney Announces $49 Million Settlement With Biotech Testing Company For Fraudulent Billing And Kickack Practices', (23 Jul. 2020), available at https://media.defense.gov/2020/Jul/28/2002465759/-1/-1/1/200723_ACTING%20MANHATTAN%20U.S.%20ATTORNEY%20ANNOUNCE._.PDF; DOJ press release, 'Acting Manhattan U.S. Attorney Announces $40.5 Million Settlement With Durable Medical Equipment Provider Apria Healthcare For Fraudulent Billing Practices', (21 Dec. 2020), available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-405-million-settlement-durable-medical-equipment.

© Law Business Research 2021

judgments and orders totalling approximately US$4.68 billion in disgorgement and penalties – an SEC record.[9]

In 2018, the DOJ issued a policy emphasising the importance of prosecuting individuals and discouraging 'disproportionate enforcement of laws by multiple authorities'. The policy provided that prosecutors should 'avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture' against a corporate being investigated by multiple enforcement authorities.[10] The policy requires DOJ lawyers from all departments to coordinate internally and, when possible, with 'other federal, state, local, or foreign enforcement authorities' to curb the practice of 'piling on' fines and penalties, 'with the goal of achieving an equitable result'.[11] Although it is difficult to measure the impact of these policies in practice, US authorities have continued to bring actions with multiple regulators and serious financial ramifications. Accordingly, corporates and individuals facing enforcement action should be mindful of the potential consequences and the opportunities to manage and reduce the ultimate fines and penalties.

26.2 Standard criminal fines and penalties available under federal law

26.2.1 Financial penalties

Many federal statutes contain their own fining provisions, which typically include a maximum fine amount. Additionally, for some crimes, the Alternative Fines Act provides for an alternative maximum fine of double the gross gain

9 Securities and Exchange Commission (SEC), Division of Enforcement 2020 Annual Report, available at https://www.sec.gov/files/enforcement-annual-report-2020.pdf.

10 Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).

11 The policy sets out various factors that should be considered when coordinating between multiple DOJ units or enforcement authorities, including 'the egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department, separate from any such disclosures and cooperation with other relevant enforcement authorities'. (Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).) An example of this policy in action can be found in the Department's March 2019 US$850 million settlement with MTS and related SEC settlement carrying a civil penalty of US$100 million. According to a press release: 'Consistent with Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (Justice Manual 1-12.100), the Department of Justice agreed to credit the civil penalty paid to the SEC as part of its agreement with MTS. Thus, the combined total amount of criminal and regulatory penalties paid by MTS and [its subsidiary] to U.S. authorities will be $850 million.' (DOJ press release, 'Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter Into Resolutions of $850 Million with the Department of Justice for Paying Bribes In Uzbekistan' (7 Mar. 2019), available at https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.)

© Law Business Research 2021

(or gross loss caused to another) from the unlawful activity.[12] Where a fine is imposed against an officer, director, employee, agent or shareholder of a corporate issuer, the fine may not be paid, directly or indirectly, by the corporate issuer.[13]

For certain offences, the DOJ may also seek criminal or civil forfeiture, or both, of property that constitutes, or is derived from proceeds traceable to, the offence.[14] Recent examples of forfeiture include (1) nearly US$1.1 billion in assets recovered in connection with various forfeiture cases related to the international money laundering and bribery scheme involving the Malaysian sovereign wealth fund 1MDB,[15] and (2) more than US$54 million forfeited in 2020 related to the DC Solar Ponzi scheme where at least half of the solar generators claimed to have been manufactured by the defendant did not actually exist.[16]

Defendants may also be required to pay restitution, taking into consideration the amount of loss sustained by each victim, the financial resources of the defendant and any other factors the court deems appropriate.[17]

Although corporates may attempt to reduce the amount of financial fines or penalties by claiming an inability to pay, the DOJ closely scrutinises any such arguments. In October 2019, the DOJ issued a non-binding policy memorandum to Criminal Division attorneys that provides 'guidance and an analytical framework' on evaluating a company's ability to pay a criminal fine

12 See 18 U.S.C. § 3571; *Southern Union Co. v. United States*, 132 S.Ct. 2344, 2350-52 (2012).

13 15 U.S.C. § 78ff(c)(3).

14 See, e.g., 18 U.S.C. § 982(a) (in connection with sentencing persons convicted of certain federal offences, including money laundering and other financial crimes, courts shall order criminal forfeiture of property 'involved in such offense, or any property traceable to such property'); 18 U.S.C. § 981(a) (property involved in certain federal offences, including money laundering and other financial crimes, 'or any property traceable to such property', is subject to civil forfeiture). Under civil forfeiture statute 18 U.S.C. § 981(a)(1)(C), property relating to a 'specified unlawful activity' as defined in 18 U.S.C. § 1956(c)(7) is subject to civil forfeiture. Among the 'specified unlawful activities' listed in 18 U.S.C. § 1956(c)(7) are racketeering, bribery of a public official, fraud by or against a foreign bank, export control violations and violations of the FCPA. Further, 28 U.S.C. § 2461(c) 'permits the government to seek *criminal* forfeiture whenever civil forfeiture is available *and* the defendant is found guilty of the offense'. *United States v. Newman*, 659 F.3d 1235, 1239 (9th Cir. 2011) (original emphasis).

15 DOJ press release, 'United States Reaches Settlement to Recover More Than $49 Million Involving Malaysian Sovereign Wealth Fund' (6 May 2020), available at https://www.justice.gov/opa/pr/united-states-reaches-settlement-recover-more-49-million-involving-malaysian-sovereign-wealth.

16 DOJ press release, 'Court-Orders Final Forfeiture of Over $54 Million in Connection with Billion Dollar Ponzi Scheme' (15 April 2020), available at https://www.justice.gov/usao-edca/pr/court-orders-final-forfeiture-over-54-million-connection-billion-dollar-ponzi-scheme.

17 18 U.S.C. § 3663(a)(1)(B)(i).

© Law Business Research 2021

or criminal monetary penalty when inability to pay is claimed.[18] The memo sets forth various legal considerations and relevant factors to take into account into account if legitimate questions remain after an analysis of an inability-to-pay questionnaire. These factors include background on current financial position, alternative sources of capital, collateral consequences and victim restitution considerations.

26.2.2 United States Sentencing Guidelines

Federal courts in the United States use the United States Sentencing Guidelines (the Sentencing Guidelines) as guidance in considering the aggravating and mitigating circumstances of a crime and imposing a sentence. These apply to both corporates and individuals. Although district courts must consult the Sentencing Guidelines, judges are not required to impose sentences – either prison terms or fines – within Guidelines ranges.[19] A recent study, in fact, suggests that federal trial judges 'now follow the advisory fraud guideline range in less than half of all cases', providing for sentences 'well below the fraud guideline'.[20]

For corporates, the calculation of the applicable fine under the Sentencing Guidelines is made by (1) identifying a 'base fine',[21] (2) identifying the minimum and maximum multipliers that combined with the base fine create a 'fine range'[22] and (3) considering whether any factors warrant any adjustments, upwards or downwards, to the fine range.[23]

In calculating the base fine under the Sentencing Guidelines, the first step is to identify the 'offence level', which depends on the characteristics of the crime. The 'base offence level' is set according to the nature of the conduct or the statute violated, and then the overall offence level will increase or decrease depending on certain factors.[24] For example, factors that may affect the overall offence level for a violation under the Foreign Corrupt Practices Act (FCPA) include the number of bribes, the amount involved and the position of the foreign official receiving the payment or benefit.[25] The total offence level helps to determine the

18 DOJ, Criminal Division, Memorandum on Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty (8 October 2019), https://www.justice.gov/opa/speech/file/1207576/download.

19 The Sentencing Guidelines were mandatory until the Supreme Court's decision in *United States v. Booker*, 543 U.S. 220 (2005).

20 Mark Bennett, Justin Levinson and Koichi Hioki, 'Judging Federal White-Collar Fraud Sentencing: An Empirical Study Revealing the Need for Further Reform', *Iowa Law Review*, 989, Vol. 102:939 (2017); George Pierpoint, 'Is white-collar crime treated more leniently In the US?', BBC News (11 Mar. 2019), available at https://www.bbc.co.uk/news/world-us-canada-47477754.

21 United States Sentencing Commission, Guidelines Manual (Guidelines Manual), § 8C2.4.

22 Id., §§ 8C2.6, 8C2.7.

23 Id., §§ 8C4.1-8C4.11.

24 Base offence levels are set out in Chapter Two of the Guidelines Manual.

25 Guidelines Manual, §§ 2C1.1(b)(1)-(3).

© Law Business Research 2021

base fine, which is the greatest of the amount specified in a table that translates the offence level into a base fine, the pecuniary gain to the organisation from the offence, or the pecuniary loss from the offence caused by the organisation, 'to the extent the loss was caused intentionally, knowingly, or recklessly'.[26]

The second step is to calculate the 'culpability score', which yields the minimum and maximum multipliers to be applied to the base fine. The culpability score is based on the characteristics of the defendant. Relevant factors may include the size of the organisation and the degree of participation in, or tolerance of, the wrongdoing; the defendant's prior criminal history; whether the defendant has violated an order or injunction, or violated a condition of probation by committing similar misconduct to that for which probation was ordered; obstruction of justice; the existence of an effective compliance programme; and self-reporting, co-operation and acceptance of responsibility.[27] The potential multipliers can range from 0.05 (a reduction of 20 times the base fine) to 4.0 (four times the base fine), depending on the culpability score. The fine range reflects the minimum and maximum multipliers as applied to the base fine. In addition to the fine, any gain to the corporate from an offence that is not otherwise part of the corporate's restitution or remediation is subject to disgorgement.[28]

Finally, the Sentencing Guidelines allow for adjustments from the fine range. This may include a reduction for substantial assistance to the government in its investigation of others[29] or remedial costs that exceed the gain to the corporate.[30] Unlike the factors that are considered for calculating the offence level and culpability score, the detriments or benefits that result from adjustments are not quantified. The court in its discretion imposes a fine within the fine range, or above or below the range. For negotiated resolutions, a corporate, through its counsel, will often negotiate the fine range with the government.

Civil penalties 26.3

Civil monetary remedies can include penalties, disgorgement and prejudgment interest. Each of these has a different purpose and method of calculation.

The SEC may impose civil monetary penalties on any person who violates or causes a violation of the securities laws. For example, the Securities Act of 1933 and the Securities Exchange Act of 1934 authorise three tiers of civil penalties, and the civil penalties imposed under these statutes can range from under US$10,000 to over US$1 million, per violation, after adjusting for inflation. Less serious civil violations fall into the first tier, where the penalty is no more than US$9,753 for an individual or US$97,523 for a corporate for

26 Id., § 8C2.4.

27 Id., § 8C2.5.

28 Id., § 8C2.9.

29 Id., § 8C4.1.

30 Id., § 8C4.9.

© Law Business Research 2021

'each act or omission' violating the federal securities laws. The second tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement, for which the maximum penalty is US$97,523 for individuals and US$487,616 for corporates, again for each act or omission. Finally, the third tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement that also directly or indirectly resulted in 'substantial losses . . . to other persons' or 'substantial pecuniary gain to the person who committed the act or omission'.[31] Third-tier penalties have a limit of US$195,047 for individuals and US$975,230 for corporates, for each act or omission.[32] The SEC sometimes asserts that the defendant's conduct involved multiple violations and seeks a penalty for each violation. Therefore, in addition to determining the relevant tier, courts generally consider whether the conduct alleged constituted multiple violations. Civil penalties for insider trading depend on the amount of the profits generated by the illicit trading. A district court can order civil penalties up to three times the profit gained or loss avoided by the violative trade.[33]

The amount of penalties sought in resolved actions against corporates depends, in part, on how the SEC's leadership uses its discretion. A 2006 policy issued under the G W Bush administration, for example, emphasised the importance of avoiding further harm to shareholders by issuing penalties. Under its current leadership, though, the SEC is expected to aggressively seek penalties and emphasise deterrence. For example, Caroline Crenshaw, one of the current commissioners, delivered a speech in March where she criticised the SEC's historical approach to penalties as 'fundamentally flawed' and called for a reconsideration of the 2006 statement on penalties.[34] She argued that 'corporate penalties should be tied to the egregiousness of the actual misconduct – not just the benefit for impact on the shareholders' and claimed that her focus would be on 'vigorous enforcement of [the] existing laws and regulations' and 'ensuring that the violator pays the price'.[35] Crenshaw outlined other factors to be considered, including, self-reporting, co-operation, remediation, the extent of harm to the victim, pervasiveness or complicity within the organisation

31 15 U.S.C. § 78u-2(b); 17 C.F.R. § 201.1001 and SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of 15 January 2021)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm (effective 15 January 2021). The maximum civil penalty amounts noted above are for violations after 2 November 2015. Maximum civil penalty amounts will be adjusted annually for inflation, as described in 17 C.F.R. § 201.1001.

32 Id.

33 15 U.S.C. § 78u-1(a).

34 SEC speech, Caroline Crenshaw, 'Moving Forward Together – Enforcement for Everyone' (9 Mar. 2021), available at https://www.sec.gov/news/speech/crenshaw-moving-forward-together.

35 Id. (emphasis removed).

© Law Business Research 2021

and the difficulty of detecting the violations.[36] It is likely that a majority of commissioners echo Crenshaw's views and will follow these considerations when imposing penalties. [37]

The DOJ likewise may seek civil penalties in certain types of matters, such as violations of federal financial, health, safety, civil rights and environmental laws.[38] For example, in January 2021, Insitu Inc agreed to pay US$25 million to resolve allegations it violated the False Claims Act by knowingly submitting materially false cost and pricing data in relation to the supply of unmanned aerial vehicles to the military.[39]

Disgorgement and prejudgment interest 26.4

The SEC and the DOJ may also seek disgorgement to prevent an entity or individual from profiting from illegal conduct and to deter subsequent misconduct.[40] Disgorgement has often accounted for a significant portion of the overall enforcement sanction. For example, in July 2020, pharmaceutical company Alexion Pharmaceuticals Inc agreed to pay more than US$21 million to settle allegations that it had violated the FCPA, of which over US$14 million was disgorgement, as compared with approximately US$3.7 million in prejudgment interest and a US$3.5 million penalty.[41] Disgorgement can also be sought in certain circumstances even when the DOJ declines to prosecute the corporate under its Corporate Enforcement Policy. For example, in 2019, it declined

36 Id.

37 Soyoung Ho, 'Swift Change in SEC Enforcement Under Biden Administration', Thomson Reuters (11 Aug. 2021), available at https://tax.thomsonreuters.com/news/swift-change-in-sec-enforcement-under-biden-administration/.

38 See, e.g., 12 U.S.C. § 1833a (providing a civil money penalty provision to the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 which allows the DOJ to seek civil penalties against persons who violate one of 14 enumerated statutes); 42 U.S.C. § 3614(d)(1)(C) (allowing it to seek civil penalties for violations of the Fair Housing Act 1968).

39 DOJ press release, 'Insitu Inc. to Pay $25 Million to Settle False Claims Act Case Alleging Knowing Overcharges on Unmanned Aerial Vehicle Contracts' (12 Jan. 2021), available at https://www.justice.gov/opa/pr/insitu-inc-pay-25-million-settle-false-claims-act-case-alleging-knowing-overcharges-unmanned.

40 See *SEC v. Huffman*, 996 F.2d 800, 802 (5th Cir. 1993); *SEC v. Cavanaugh*, 445 F.3d 105, 117 (2d Cir. 2006) (noting that disgorgement 'has the effect of deterring subsequent fraud'); DOJ press release, 'Deutsche Bank Agrees to Pay over $130 Million to Resolve Foreign Corrupt Practices Act and Fraud Case' (8 Jan. 2021), available at https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-over-130-million-resolve-foreign-corrupt-practices-act-and-fraud (including US$681,480 in criminal disgorgement).

41 DOJ press release, 'Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges' (29 Mar. 2019), available at https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve; SEC press release, 'SEC Charges Medical Device Company With FCPA Violations' (29 Mar. 2019), available at https://www.sec.gov/news/press-release/2019-48.

© Law Business Research 2021

to prosecute Cognizant Technology Solutions for violations of the FCPA, yet the company agreed to pay nearly US$20 million in disgorgement, which represented 'all profits fairly attributable to the bribery conduct'.[42]

In 2021, Congress made several important changes to the US securities laws that will impact the SEC's ability to recover funds though disgorgement. Specifically, Congress passed a provision titled 'Investigations and Prosecution of Offenses for Violations of the Securities Laws'.[43] This provision amended certain disgorgement-related provisions of the Securities Exchange Act of 1934 to (1) expressly grant the SEC statutory authority to pursue disgorgement as a remedy for civil enforcement actions in federal court, (2) extend the statute of limitations for all disgorgement actions involving fraud and scienter from five years to 10 years, and (3) direct courts to apply a 10-year statute of limitations for all other claims seeking equitable remedies, such as injunctions, bars, suspensions, and cease and desist orders. Therefore, with this legislation, Congress has greatly expanded the time frame in which the SEC can seek disgorgement, also increasing the total disgorgement the SEC can collect.

This legislation was perceived by many to be a reaction to the US Supreme Court's recent decisions in *Kokesh* and *Liu*. In *Kokesh v. SEC*, the US Supreme Court had held in 2017 that the SEC's disgorgement remedy was subject to a strict five-year statute of limitations, explaining that '[d]isgorgement in the securities-enforcement context is a "penalty" . . . and so disgorgement actions must be commenced within five years of the date the claim accrues'.[44] Following the US Supreme Court's ruling in *Kokesh*, this statute of limitations had significantly impacted the SEC's ability to obtain disgorgement. Indeed, in its 2019 annual report, the SEC estimated that the Kokesh ruling had 'caused the [SEC] to forgo approximately $1.1 billion in disgorgement in filed cases'.[45]

The new legislation also addressed, at least in part, potential limitations to the SEC's disgorgement powers from a June 2020 Supreme Court case, *Liu v. SEC*. There, the Court held that the SEC could continue to seek disgorgement pursuant to its power to award 'equitable relief' under Section 21(d)(5) of the Securities Exchange Act but also held that the SEC could only do so where the disgorgement sought does not exceed the defendant's net profits and is awarded for victims. In doing so, the majority, without reaching any conclusions, also raised the possibility that disgorgement awards may not be an equitable remedy – and therefore not allowed under the relevant statute – in situations where courts decline to deduct expenses from the award, impose joint-and-several liability or fail to return money to investors. With its

42 DOJ Declination Letter, 'Re: Cognizant Technology Solutions Corporation' (13 Feb. 2019), available at https://www.justice.gov/criminal-fraud/file/1132666/download.

43 William M (Mac) Thornberry, National Defense Authorization Act for Fiscal Year 2021, available at https://www.congress.gov/bill/116th-congress/house-bill/6395/text?r=8&s=1.

44 *Kokesh v. SEC*, 137 S.Ct. 1635, 1639 (2017).

45 SEC, Division of Enforcement Annual Report (2019), available at https://www.sec.gov/files/enforcement-annual-report-2019.pdf.

© Law Business Research 2021

legislation, though, Congress confirmed the SEC's ability to obtain disgorgement even where money is not distributed to investors. However, notwithstanding the 2021 legislation, some of the residual questions in *Liu* remain unresolved, meaning open questions related to the SEC's enforcement abilities will continue to be addressed by courts.

Beyond disgorgement, the SEC also generally obtains prejudgment interest on any disgorgement amount. The rules that apply to administrative proceedings brought by the SEC require that such amounts be included in any disgorgement.[46] District courts presiding over actions generally may determine whether prejudgment interest is appropriate.[47] The interest rate applied is typically the 'underpayment' rate set by the IRS.[48] There is no single approach for measuring when the clock begins to run on interest calculations. In some cases, it has been measured from the date the ill-gotten funds were received, up to the date of judgment.[49] In others, it may run from multiple dates where the matter involves multiple transactions,[50] or, where the applicable dates are difficult to identify, from the date of the complaint.[51]

Injunctions 26.5

The DOJ may also seek affirmative relief through an injunction where it is deemed necessary to advance public interests or enforce government functions. Such injunction actions may be specifically provided for by statute, may be used to enforce statutes that do not specifically provide for injunctive relief or may be sought from an appellate court pursuant to the All Writs Act.[52]

Likewise, the SEC may seek either a preliminary or permanent injunction when it appears that a person is engaged in, or is about to engage in, acts

46 17 C.F.R. § 201.600(a).

47 *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1476 (2d Cir. 1996).

48 Id., 101 F.3d at 1476 (citing SEC Rules and Regulations, 60 Fed. Reg. 32738, 32788 (23 Jun. 1995)). See also 17 C.F.R. § 201.600(b). The underpayment rate charged by the IRS is three percentage points above the federal short-term rate and for purposes of calculating interest on sums disgorged is compounded quarterly. 26 U.S.C. § 6621(a)(2); 17 C.F.R. § 201.600(b).

49 *SEC v. DiBella*, 2008 WL 6965807 at *3 (D. Conn. 18 July 2008); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 Feb. 2009) ('The time frame for the imposition of prejudgment interest usually begins with the date of the unlawful gain and ends at the entry of judgment.') (quoting *SEC v. Yun*, 148 F. Supp. 2d 1287, 1293 (M.D. Fla. 2001).

50 S*EC v. Savino*, 2006 WL 375074 at *18 & n.10 (S.D.N.Y. 16 Feb. 2006) (calculating interest from the first day of the month following each improper trade).

51 *SEC v. United Energy Partners, Inc.*, 2003 WL 223392 at *2 n.12 (N.D. Tex. 28 Jan. 2003), aff'd, 88 F. App'x 744 (5th Cir. 2004) (using date of complaint for accrual of prejudgment interest award where dates on which defendant acquired disgorged funds were not clear); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 Feb. 2009) (same).

52 28 U.S.C. § 1651(a). See US Department of Justice Civil Resource Manual, 'Injunctions', available at https://www.justice.gov/jm/civil-resource-manual-214-injunctions.

© Law Business Research 2021

or practices constituting a violation of the securities laws.[53] For example, in March 2020, the SEC obtained a preliminary injunction barring the company Telegram from delivering digital tokens called Grams, after the court held that the SEC had shown there was a sufficient likelihood that Telegram's sales were part of a larger scheme to unlawfully distribute the Grams.[54]

26.6 Other consequences

In addition to the criminal and civil penalties noted above, defendants may face other consequences as a result of a US criminal or civil action. For one, defendants may also face civil and criminal forfeiture of assets, including real and personal property constituting, or derived from proceeds traceable to, a violation, or to a conspiracy to commit a violation.[55] For certain offences, courts are required to order that property traceable to an offence be forfeited.[56]

See Chapters 18 on individuals in cross-border proceedings and 31 on individual penalties

Further, investigation or prosecution by authorities in one jurisdiction may also lead to investigations, prosecutions or resolution short of prosecution by authorities in other jurisdictions. For example, in January 2020, the largest foreign bribery settlement to date was entered into between airplane manufacturer Airbus and authorities in France, the United Kingdom and the United States. Airbus agreed to pay combined penalties of over US$3.9 billion to resolve anti-corruption and export control violations.[57] It is expected that this trend of multinational investigations and co-operation across jurisdictions will continue in the coming years.

See Chapter 24 on negotiating global settlements

Defendants may also face a variety of actions from other US government agencies, international organisations, other corporates or even shareholders and employees, actions which may involve additional litigation and other monetary penalties or debarment. These 'tag along' actions can even arise from investigations of unrelated conduct that are assisted by co-operation clauses required by prior settlements.[58]

---

53 15 U.S.C. § 77t(b); 15 U.S.C. § 78u(d).

54 SEC press release, 'Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges' (26 Jun. 2020), available at https://www.sec.gov/news/press-release/2020-146.

55 See 18 U.S.C. §§ 981, 982; 28 U.S.C. § 2461.

56 See 18 U.S.C. § 982. Examples of offences where forfeiture is required include, but are not limited to, laundering of monetary instruments under 18 U.S.C. § 1956, engaging in monetary transactions derived from specified unlawful activity under 18 U.S.C. § 1957, receipt of commissions or gifts for procuring loans under 18 U.S.C. § 215 and fraud by wire, radio, or television under 18 U.S.C. § 1343.

57 See DOJ press release, 'Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (31 Jan. 2020), available at https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

58 For example, in 2016, Odebrecht entered into a plea agreement with the DOJ for FCPA violations requiring it to co-operate fully with investigations conducted by multilateral development banks. On 29 January 2019, the World Bank debarred Odebrecht SA's

© Law Business Research 2021

In addition, in connection with certain types of enforcement actions, such as FCPA enforcement, money laundering and sanctions violations, corporates may also be required to retain corporate compliance monitors. For example, in May 2021, State Street Corporation entered into a two-year deferred-prosecution agreement pursuant to which it agreed not only to pay a US$115 million criminal penalty but also to retain an independent corporate compliance monitor for two years.[59]

See Chapter 33 on monitorships

Finally, in some circumstances, individuals or entities may be barred or suspended from doing business with the executive branch of the United States government.[60] Debarment may be triggered by a criminal conviction or, in some circumstances, even an adverse civil judgment, and applies to all subdivisions of a corporation unless the decision is limited by its terms to specific divisions or organisational units.[61] Suspension may occur upon adequate evidence that certain wrongdoing was committed and when it is in the public's interest.[62] Like debarment, suspension affects all organisational divisions of a corporation, unless otherwise specified.[63]

Remedies under specific statutes 26.7

By way of example, the fines, penalties and other remedies associated with particular federal criminal statutes of potential interest are outlined below.

Foreign Corrupt Practices Act 26.7.1

The FCPA criminalises bribery of foreign officials, either directly or through an intermediary, to obtain business or some other benefit. Its anti-bribery provisions apply not only to all US corporates and persons, but also can apply to foreign corporates that issue securities within the United States or file certain reports with the SEC (issuers) and to these issuers' officers and employees, among others. The FCPA also criminalises actions taken in the United States by foreign corporates or their agents that are in furtherance of an improper

Brazilian construction and engineering subsidiary for three years, crediting '[d]isclosures from prior settlements' as contributing to the World Bank's investigation. Plea Agreement, United States District Court E. Dist. of NY against Odebrecht S.A., Cr. No. 16-643 (RJD) (21 Dec. 2016), at 11, available at https://www.justice.gov/opa/press-release/file/919916/download; World Bank Group Sanctions System Annual Report FY19, at 20, available at http://documents1.worldbank.org/curated/en/980641572096094561/pdf/World-Bank-Group-Sanctions-System-Annual-Report-FY19.pdf.

59 See DOJ press release, 'State Street Corporation to Pay $115 Million Criminal Penalty and Enter Into Deferred Prosecution Agreement in Connection With Scheme to Overcharge Custody Customers' (13 May 2021), available at https://www.justice.gov/usao-ma/pr/state-street-corporation-pay-115-million-criminal-penalty-and-enter-deferred-prosecution.

60 48 C.F.R. §§ 9.406-1(c), 9.407-1(d).

61 48 C.F.R. §§ 9.406-1(b), 9.406-2(a).

62 48 C.F.R. §§ 9.407-1(a), 9.407-2(a).

63 48 C.F.R. § 9.407-1(c).

© Law Business Research 2021

payment or offer. Further, the FCPA's books and records and internal controls provisions also require corporates whose securities are listed in the United States or who file reports with the SEC to keep accounting records that accurately reflect the corporate's transactions and to maintain a system of internal controls.[64]

Violations of the FCPA can result in heavy penalties. For one, corporate entities may be subject to financial penalties of up to US$2 million per violation of the FCPA's anti-bribery provisions,[65] US$25 million per violation of the FCPA's accounting provisions,[66] or up to twice the gross pecuniary gain or loss from the violation pursuant to the Alternative Fines Act.[67] In addition, civil penalties for FCPA anti-bribery and accounting provisions violations may apply.[68]

Further, certain individuals may be either fined up to US$100,000 (US$250,000 under the Alternative Fines Act or twice the gain or loss from the violation) or imprisoned for up to five years, or both, for a criminal violation of the FCPA's anti-bribery provisions.[69] For criminal violations of the FCPA's accounting provisions, certain individuals can be subject to a fine of up to US$5 million or imprisonment for up to 20 years, or both.[70] Individuals may also face civil penalties for FCPA anti-bribery and accounting provisions violations.[71] Issuers, as defined under the FCPA, are prohibited from paying these individuals' criminal and civil fines.[72]

Moreover, the DOJ may also bring a civil action to seek an injunction against domestic concerns and persons other than issuers to prevent a current or imminent FCPA violation.[73] Likewise, the SEC may seek injunctions to prevent FCPA violations from occurring.[74]

In addition, disgorgement is often a key component of a civil FCPA esolution. For example, in October 2020, Goldman Sachs agreed to pay the DOJ and SEC more than US$2.9 million to resolve FCPA charges related to the

64 15 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a), 78(m).

65 15 U.S.C. §§ 78dd-2(g)(1)(A), 78 dd-3(e)(1)(A), 78ff(c)(1)(A).

66 15 U.S.C. § 78ff(a).

67 18 U.S.C. § 3571 (c)(2), (d).

68 15 U.S.C. §§ 78ff(c)(1)(B), 78u(d)(3); 17 C.F.R. § 201.1001; SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

69 15 U.S.C. §§ 78dd-2(g)(2), 78dd-3(e)(2); 18 U.S.C. § 3571 (b)(2), (b)(3), (d).

70 15 U.S.C. § 78ff(a).

71 15 U.S.C. §§ 78ff(c)(2)(B), 78u(d)(3); 17 C.F.R. § 201.1001; SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

72 15 U.S.C. § 78ff(c)(3).

73 15 U.S.C. §§ 78dd-2(d), 78dd-3(d).

74 15 U.S.C. § 78u(d)(1).

© Law Business Research 2021

1MDB bribery scheme. Of the total amount paid by Goldman Sachs to settle the SEC charges (more than US$1 billion), US$606.3 million was disgorgement.[75] However, as discussed above in detail, the SEC's use of disgorgement in civil actions has been limited by the Supreme Court's decision in *Liu v. SEC*.[76]

For corporates seeking to avoid the heaviest penalties, however, the FCPA Corporate Enforcement Policy establishes a presumption that, 'absent aggravating circumstances' such as involvement by executive management in the misconduct or significant profit to the corporate from the misconduct, a corporate will receive a declination if it 'has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated'. Moreover, even if aggravating circumstances are present, for a corporate that voluntarily self-discloses, fully co-operates and timely and appropriately remediates, the DOJ will still recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines fine range, except in the case of a recidivist.[77]

On 20 November 2019, the FCPA Corporate Enforcement Policy was amended to clarify that a corporate that voluntarily discloses misconduct need not disclose 'all relevant facts known to it', but simply 'all relevant facts known to it at the time of the disclosure'. In addition, the new policy explains that, for a corporate to fully co-operate, it must identify 'relevant evidence not in the company's possession' that the corporate is aware of.[78] However, the corporate is no longer required to identify opportunities 'to obtain relevant evidence not in the company's possession and not otherwise known to the Department' that the corporate 'is or should be aware of'.[79]

Federal criminal money laundering 26.7.2

The principal federal criminal money laundering statutes are 18 USC Sections 1956 and 1957. Section 1956 generally prohibits a person from knowingly engaging in financial transactions with the proceeds of certain unlawful activities to promote further unlawful activity, concealing the proceeds, evading taxes or avoiding reporting requirements. Section 1957 also prohibits a person from knowingly engaging in a monetary transaction involving property valued at more than US$10,000 that derives from specified unlawful activities. In regard

75 SEC press release, 'SEC Charges Goldman Sachs With FCPA Violations' (22 Oct. 2020), available at https://www.sec.gov/news/press-release/2020-265.

76 *Liu v. SEC*, No. 18-1501, 2020 WL 3405845, (U.S. 22 Jun. 2020).

77 DOJ, FCPA Corporate Enforcement Policy, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

78 Id. On 3 July 2020, the DOJ and the SEC issued the first comprehensive update to the FCPA Resource Guide since it was first published in 2012, which now includes a section on the FCPA Corporate Enforcement Policy. A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition, at 51 (Jul. 2020), available at https://www.justice.gov/criminal-fraud/file/1292051/download.

79 DOJ, FCPA Corporate Enforcement Policy (updated March 2019), available at https://www.justice.gov/criminal-fraud/file/838416/download.

© Law Business Research 2021

to both sections, the specified unlawful activities include proceeds resulting from offences involving bribery of a foreign official, fraud by or against a foreign bank, and certain smuggling and export control violations, to name a few.[80]

See Chapters 18 on individuals in cross-border proceedings and 31 on individual penalties

Any violation of Section 1956 is punishable by imprisonment for not more than 20 years, a fine of up to US$500,000 or twice the value of the property involved, or both. In addition, such violations can incur a civil penalty up to the greater of US$10,000 or the value of the property involved in the offence, plus asset forfeiture. For Section 1957, the maximum penalty is 10 years' imprisonment or a fine of up to twice the value of the property involved, or both.[81]

26.7.3 Export controls and trade sanctions

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces most US economic sanctions. However, the US Commerce Department's Bureau of Industry and Security and DOJ National Security Division also enforce some aspects of US sanctions. Generally, these sanctions, such as the blocking of assets and trade restrictions, are used to accomplish national security and foreign policy objectives.

The sanctions can be either comprehensive for a jurisdiction, such as Cuba,[82] or targeted to particular individuals and entities, such as the sanctions imposed on one Chinese government entity and specific officials pursuant to the global Magnitsky Human Rights Accountability Act.[83] Typically, US sanctions either restrict activities that take place in the US or restrict activities that involve a 'US person', generally defined widely to include US citizens, permanent residents, persons present in the United States, and corporates organised under the laws of the United States or any jurisdiction therein, as well as those corporates' foreign branches.[84] However, non-US persons and corporates can face penalties under US sanctions as well, including for 'causing' a violation by a US person.[85] For example, in 2019, OFAC entered into a settlement with British Arab Commercial Bank plc, a UK-based commercial bank, in part for causing US financial institutions to engage in prohibited conduct involving Sudan.[86]

Fines for violations of the sanctions regulations can be significant. As of 18 August 2021, OFAC had settled 11 enforcement actions, with civil penalties

80 18 U.S.C. §§ 1956, 1957.

81 Id.

82 Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 Sep. 2018).

83 Department of the Treasury, 'Treasury Targets Iranian-Backed Hizballah Officials for Exploiting Lebanon's Political and Financial System' (9 Jul. 2019), available at https://home.treasury.gov/news/press-releases/sm724.

84 See, e.g., 31 C.F.R. §§ 560.312, 560.314.

85 See, e.g., 50 U.S.C. § 1705(a).

86 Department of the Treasury, 'Settlement Agreement' (Jul. 2017), available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/transtel_settlement.pdf.

© Law Business Research 2021

totalling more than US$15 million in 2021.[87] And in 2020, it settled 16 enforcement actions for just over US$23.5 million.[88] Criminal penalties for wilful violations of OFAC sanctions can include fines ranging up to US$1 million per violation or imprisonment of up to 20 years, or both.[89] Under Title 18, Section 3571, the government can also pursue fines and penalties against an organisation of up to US$500,000 or twice the pecuniary gain or loss derived from the offence, as well as forfeiture under 18 USC Section 981. Further, penalties for violations of the Trading with the Enemy Act, which provides the statutory authority for the Cuba sanctions, can be up to US$90,743 per violation (which may be adjusted for inflation), and criminal penalties can reach US$1 million.[90] Financial penalties for violations of the International Emergency Economic Powers Act, which underlies other sanctions programmes, are also possible; associated civil penalties can be up to US$250,000 or twice the amount of the unlawful transaction, and criminal penalties permit a fine of up to US$1 million and imprisonment of up to 20 years.[91]

See Chapter 45 on sanctions

Racketeer Influenced and Corrupt Organizations Act 26.7.4

The Racketeer Influenced and Corrupt Organizations Act (RICO) provides criminal penalties as well as a civil, private cause of action for acts performed as part of a criminal organisation or enterprise.[92] The statute contains variations on the proscribed conduct but generally criminalises participation in an 'enterprise' in interstate or foreign commerce through a 'pattern of racketeering

87 Department of the Treasury, '2021 Enforcement Information', available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

88 Department of the Treasury, '2020 Enforcement Information', available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2020-enforcement-information.

89 See, e.g., 50 U.S.C. § 1705(c).

90 31 C.F.R. § 501.701; Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 Sep. 2018) (extending the expiration of Cuba sanctions pursuant to the Trading with the Enemy Act until September 2019).

91 50 U.S.C. § 1705; 31 C.F.R. § 501; Congressional Research Service, 'The International Emergency Economic Powers Act: Origins, Evolution, and Use' (20 Mar. 2019), available at https://fas.org/sgp/crs/natsec/R45618.pdf.

92 18 U.S.C. §§ 1961, et seq.

© Law Business Research 2021

activity'.[93] Such racketeering activity includes mail and wire fraud and money laundering violations under Sections 1956 and 1957, as outlined above.[94]

RICO violations are punishable by fines and imprisonment for up to 20 years, plus forfeiture of any interest acquired or maintained through the violation, any interest in any enterprise that was established, operated, controlled, conducted or participated in as part of the RICO violation (or the property of such an enterprise) and any property constituting or derived from any proceeds that the person obtained, directly or indirectly, from racketeering activity.[95]

Additionally, the government may seek pre-indictment restraining orders for the purpose of preventing defendants from transferring assets the government may potentially seek to have forfeited. To obtain such an order, the government must establish that (1) there is a substantial probability that it will prevail on the forfeiture issue, (2) property will be destroyed or placed beyond the court's reach without the order and (3) the need to maintain the property's availability outweighs the hardship of a restraining order. Pre-indictment restraining orders are effective for 90 days, but can be extended for good cause or as a result of the filing of an information or indictment.[96]

There are also civil remedies under RICO available to any person injured by a RICO defendant, which include treble damages sustained by the injured party and the cost of the lawsuit, including reasonable attorneys' fees.[97]

26.8 Conclusion

Corporates and individuals may face a variety of fines, penalties and other collateral consequences when defending against or settling an enforcement action with US authorities. As has been explained, these risks can be substantial. That said, these risks can be managed, mitigated or avoided by engaging knowledgeable external counsel, who can evaluate the situation, provide advice and thereby enable the corporate or individual to make an informed decision about how to proceed.

93 18 U.S.C. § 1962. The first variation makes it unlawful for any person who has received any income derived from a pattern of racketeering activity to use any part of such income or its proceeds to acquire, establish or operate any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(a). The second variation makes it unlawful for any person to engage in a pattern of racketeering activity to acquire or maintain any interest in any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(b). The third variation makes it unlawful for any person employed by or associated with any enterprise involved in interstate or foreign commerce to conduct the enterprise's affairs through a pattern of racketeering activity. 18 U.S.C. § 1962(c). The statute also makes it unlawful for a person to conspire to participate in the conduct outlined in (a), (b) or (c). 18 U.S.C. § 1962(d).

94 18 U.S.C. § 1961(1).

95 18 U.S.C. § 1963(a).

96 18 U.S.C. § 1963(d).

97 18 U.S.C. § 1964(c).

© Law Business Research 2021

27

Global Settlements: The In-house Perspective

Claire McLeod[1]

Introduction 27.1

Reaching a global settlement will involve engagement with multiple enforcement agencies across multiple jurisdictions and co-ordination of a significant number of external and internal stakeholders. Settlements are multifaceted and require consideration of many factors, including the commercial aspects, not just the penalty but also potentially redress or compensatory payments, the collateral consequences for the company, the impact on employees, continuing regulatory requirements and potential follow-on litigation. The timing and sequencing of a global settlement with multiple agencies and regulators can also be key. One of the principal advantages for a corporate in reaching a global settlement is to achieve a resolution guaranteeing finality and certainty. If this cannot be achieved, or achieved with a high degree of certainty, a company has to consider whether the benefits of a more limited settlement outweigh a further period of uncertainty. This can be a complex and difficult decision, especially when some of the uncertainty may not be fully quantifiable. This chapter will look at these key considerations from the perspective of the different stakeholders in a global settlement.

Senior management 27.2

When considering global settlements, key considerations for senior management will include (1) the size of the financial penalty and any other financial components to the settlement, (2) the extent to which the settlement will bring

1 Claire McLeod is the head of litigation, investigations and enforcement for Europe and the Middle East at Barclays Bank PLC. The views expressed are the author's own and do not represent the views of Barclays Bank PLC.

© Law Business Research 2021

finality of resolution to the company, (3) potential collateral consequences to the company's business, and (4) reputational damage.

Although the pace of imposing financial penalties has slowed, cumulative penalties against banks in Europe and North America since 2009 total US$394 billion,[2] and there have been a number of significant penalties in the past two years. Negotiating the financial penalty of any global resolution will be a key consideration for senior management. For regulators and law enforcement agencies working within a rigid penalty framework, the scope for negotiating the proposed penalty may be more limited. For others there may be greater scope to seek a more proportionate penalty by putting forward arguments about the calculation method or the applicability of different components, for example whether disgorgement is appropriate. Ultimately, senior management will need to understand and take into account the proportionality of the penalty and the impact it will have on the company's overall financial health.

In the United Kingdom, focused resolution agreements (FRAs) allow financial services firms to challenge a penalty proposed by the Financial Conduct Authority (FCA).[3] In April 2019, the FCA fined Standard Chartered Bank just under £102.2 million for anti-money laundering breaches.[4] This case was one of the first to involve an FRA. Standard Chartered agreed the FCA's findings of fact and liability, but argued that the proposed penalty was too high. Standard Chartered challenged the size of the penalty at a hearing before the FCA's Regulatory Decisions Committee (RDC), arguing that the proposed penalty was not proportionate based on the seriousness of the relevant breaches and certain mitigating factors. The RDC found in the bank's favour, reducing the penalty from £155 million to £102 million, which included maintaining a 30 per cent settlement discount – a term of the FRA.

In addition to financial penalties, there may be a further financial component of the resolution involving significant redress, compensatory payments or consumer relief. Indeed, a regulator may require this as part of any settlement.[5] The potential for financial impacts beyond the original penalties as a result of follow-on civil litigation must also be taken into account. Management will need to understand the total financial impact across all aspects of the settlement and any consequential financial impacts before deciding whether it is in the best interests of the company and its shareholders to proceed.

A key consideration for senior management will be the extent to which the settlement will bring finality of resolution for the company. The uncertainty

2 See BCG Global Risk 2021: Building a Stronger, Healthier Bank, https://www.bcg.com/en-gb/publications/2021/embracing-change-post-pandemic-in-the-banking-industry.

3 The FCA introduced Focussed Resolution Agreements in March 2017.

4 https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls.

5 In 2017, the FCA used its powers under s.348 of the Financial Services and Markets Act to require Tesco plc and Tesco Stores Limited to pay compensation to investors for market abuse, https://www.fca.org.uk/news/press-releases/tesco-pay-redress-market-abuse.

© Law Business Research 2021

created by a significant enforcement investigation, and what the outcome, business impact and reputational damage will be, can often mean that settling with only one agency or on one aspect of the action is unlikely to be attractive. One of the main advantages to reaching a global settlement is being able to draw a line under the matter so that management can refocus their attention on their business and customers. This is not always easy to achieve. Co-ordinating a global settlement across multiple jurisdictions and agencies can be challenging, requiring the agencies synchronising the completion of their investigations and the corporate negotiating settlements simultaneously with each agency. Settling with one agency could also risk triggering an investigation by another with further (and in some cases heightened) risk to the company and additional uncertainty. In these circumstances, the company may consider it is not in its interests to seek an earlier settlement because the potential exposure and uncertainty remaining is too significant.

The likely collateral consequences of any resolution, in particular the potential impact on the company's business and customers will also be paramount. The risk of collateral consequences in recent years has become more acute as the number of corporate criminal actions has increased. These could include debarment from tendering for public procurement contracts, disqualification from – or restrictions on – specific business practices, and having to seek waivers from regulators to continue other business activities. These collateral consequences may dictate the terms on which a company is willing to enter a settlement. For example, deferred prosecution agreements (DPAs), rather than a guilty plea or conviction, could be beneficial to a company in avoiding certain collateral consequences. The DPAs entered into by Rolls-Royce in 2017 and Airbus in 2020 allowed the companies to avoid being debarred from tendering for public contracts, which was an important consideration for the judges who granted them.[6]

The potential (and often unquantifiable) reputational impact of a settlement should also not be underestimated. The company will want to plan a comprehensive strategy to minimise reputational damage. One aspect of this will be the proposed terms of the settlement, including the nature and extent of the factual and legal admissions required. Senior management will want to ensure that any admissions are supported by the evidentiary record and will want to understand if any of these admissions give rise to the risk of further regulatory

6 *Serious Fraud Office v. Rolls-Royce plc* (Case No. U20170036) [2017] Lloyd's Rep FC 249, 'Debarment and exclusion would clearly have significant, and potentially business critical, effects on the financial position of Rolls-Royce. This could lead to the worst case scenario of a very negative share price impact, and, potentially, more serious impacts on shareholder confidence future strategy, and therefore viability.' *per* Leveson P, at para. 55. The judgment in *Director of the Serious Fraud Office v. Airbus SE* (Case No: U20200108) [2020], *per* Dame Victoria Sharp, at 85–86, noted that the financial impact of debarment would exceed €200 billion and affect thousands of employees in the United Kingdom, Airbus's share price and consequently pensioners, and thousands of third-party suppliers.

© Law Business Research 2021

or enforcement action or follow-on litigation. They will also want to take into account the reputational impact. These are key considerations for a company when negotiating the terms of any final statement of facts or agreement.

Other considerations will include any longer term impact on the company of any other settlement terms, for example the installing of a monitor or imposition of probationary terms. Monitors can be extremely costly, both in terms of financial costs and management time.

Taking all these commercial aspects into account, senior management will be looking for a settlement that achieves the highest degree of finality and the least impact on the business and its customers. The extent to which the company considers it has already addressed the root causes of the issues, and will be able to reassure its customers and employees that this is the case, will be critical.

27.3 Shareholders

A global settlement has to be in the interests of, and justifiable to, a company's shareholders. Many of the considerations cited above for senior management will also be key issues for the shareholders.

Aside from the level of the penalty and the impact it will have on the company's financial position, the single biggest concern for shareholders is likely to be achieving a final resolution. Shareholders will want to see the company move on and management be able to focus their attention on the business without the distraction of an ongoing enforcement action. A partial settlement or one that may trigger other litigation or enforcement action is unlikely to be considered a good outcome.

Shareholders will also expect the company to take appropriate action against any employees involved in the misconduct and will want to see that the company has taken steps to remediate any underlying issues. They will want assurance that the misconduct will not recur. They will want to know that the company can properly move forward and draw a line under the matter.

27.4 Employees

An enforcement investigation and global resolution can have a significant and long-lasting impact on employees. In most enforcement matters involving a global organisation, the misconduct itself centres on a small part of the company, and a small number of employees. For those employees directly involved there will likely be a need to consider disciplinary proceedings and other issues such as the question of continuing to fund their legal representation and applicability of directors' and officers' liability insurance.

The majority of the company's employees, however, will know very little about the underlying issues until the settlement is announced. They will be most concerned about whether there will be any impact on them, including their ability to service their customers, and whether it will result in any changes to the structure or management of the company. Employees will also want to have confidence in senior management's handling of the matter, and the steps taken to remediate the underlying issues and prevent similar occurrences. It

© Law Business Research 2021

may also be important for employees to be able to communicate the measures taken to customers.

When a global settlement is announced, a company's management should provide sufficient information to employees to allow them to understand the rationale for the settlement, what it means in terms of reaching a final resolution, if there is going to be any impact on the company's business or customers, and, if so, how this impact will be mitigated. It is also important for employees to know what they can communicate to customers.

Despite not being involved in the underlying misconduct, the resultant negative reputational impact can still have an effect on employees, in terms of morale and motivation. It is therefore important for senior management to reassure employees that the matter has concluded, the company has taken appropriate action to address and remediate the issues, and to recognise the ongoing support and efforts of the wider employee workforce.

Customers 27.5

The single most important aspect of a global settlement for a company's customers is likely to be whether it will have any impact on the company's ability to continue servicing them. On announcement of a global settlement, customers will be looking for assurance, to the extent possible, that there will be no impact on the company's ability to continue its business. To the extent there are restrictions or constraints placed on the company's business activities by the settlement, they will want to understand how the company will minimise the impact of these. To avoid the imposition of business restrictions or suspensions by a regulator (which are generally made public), companies will often seek to voluntarily agree a variation for a limited period to minimise customer disruption. Customers will also be looking for assurance that there will be continuity of service and the least disruption possible. This may involve structuring things differently or making changes to personnel. It will be important to identify all these issues and any contingencies planned well in advance of the settlement announcement.

Some customers may also want to know what changes the company has made to address the issues. This may be particularly important to customers or counterparties who conduct business on behalf of investors or shareholders to whom they owe fiduciary duties. This may also be more significant for customers where they consider there is a risk of an impact on their own compliance and regulatory obligations, for example if the misconduct involves anti-money laundering or sanctions breaches.

Some companies have considered that the risks of doing business in certain areas or jurisdictions are too high and have withdrawn from them. This 'de-risking' has been most prevalent in the banking industry and in respect of concerns about anti-money laundering (AML) and countering the financing of terrorism (CFT), for example banks' withdrawal from business in areas such as the money transfer business sector. Although this is not surprising, there are broader socio-economic consequences, and concerns have been raised that

© Law Business Research 2021

this de-risking can in fact frustrate AML/CFT objectives by pushing higher risk transactions into more informal, unregulated channels that are harder to monitor.[7]

27.6 Regulators and enforcement agencies

The size of the monetary penalty remains a key aspect of a settlement by most regulators and enforcers.[8] Credible deterrence is seen by many to require imposing a financial penalty so severe it affects the company's cost of doing business, to deter others at the company or in the industry from committing the same misconduct. Where multiple agencies are involved, there may also be political pressure to match equivalent penalties in other jurisdictions, increasing the overall settlement figure.

Another important aspect for the agencies in reaching a global settlement is often how the company will give redress to those who have been harmed by the misconduct. If a company can demonstrate that it has voluntarily given redress for or remedied the misconduct in a timely and effective manner it is likely to receive credit for this in any final settlement. The FCA, for example, has said it will take this into account when applying sanctions, including applying heavier sanctions where steps have not been taken to address harm.[9] Similarly, in the criminal context, the Sentencing Council Guideline on Fraud, Bribery and Money Laundering Offences lists, as a mitigating factor in sentencing a corporate, whether victims have been 'voluntarily reimbursed/compensated'.[10]

The terms of any published statement of facts or final notice will also be important to make the severity and scale of the misconduct clear to the industry and wider public. The importance of this to the enforcement agency or regulator is often matched with the importance to the company, especially given the risk of follow-on litigation.

---

7 De-risking in the Financial Sector (7 Oct. 2016), https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector.

8 See, e.g., Chapter 6 of the FCA's Decision Procedure and Penalties manual, DEPP 6A.1.3. 'The principal purpose of imposing such a measure is to promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches, helping to deter other persons from committing similar breaches, and demonstrating generally the benefits of compliant behaviour.'

9 See, e.g., the FCA Mission: Approach to Enforcement, April 2019 (https://www.fca.org.uk/publication/corporate/our-approach-enforcement-final-report-feedback-statement.pdf), in which the FCA places emphasis on the importance of taking action to address harm caused by serious misconduct. See also, as an example of the FCA's approach, the Final Notice imposed on Redcentric plc in June 2020 in relation to which Mark Steward, Executive Director of Enforcement and Market Oversight, said: 'The FCA has taken into account Redcentric's approach to compensate affected shareholders, and has decided to impose a public censure rather than a financial penalty.'

10 https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/corporate-offenders-fraud-bribery-and-money-laundering/.

© Law Business Research 2021

In recent years, regulators and enforcement agencies have also placed a strong emphasis on holding individuals to account for the misconduct, both in terms of enforcement and disciplinary action. In October 2021, Deputy Attorney General Lisa Monaco announced changes to the US Department of Justice's (DOJ) policy on corporate criminal enforcement, including that to be eligible for co-operation credit, companies must provide the DOJ with all non-privileged information about individuals involved in or responsible for the misconduct, regardless of their position or seniority, and not just limited to those 'substantially involved', as per prior policies.[11] The introduction of the Senior Managers and Certification Regime by the FCA in the United Kingdom is also aimed at driving greater accountability within financial services firms, with the FCA and the UK Prudential Regulatory Authority both placing an emphasis on firms complying with requirements on *ex post* risk adjustment, to adjust variable remuneration to take into account a specific crystallised risk or adverse performance outcome including relating to misconduct.[12] In its guidance, the FCA makes it clear that it expects firms to consider applying adjustments not just to those directly involved in the misconduct but also to those employees whose roles and responsibilities include areas where failures or poor performance contributed to, or failed to prevent, the risk or misconduct.

The challenges, however, of holding both companies and individuals to account, particularly in the criminal context, have been clearly seen in a number of high-profile cases brought by the Serious Fraud Office. While it secured DPAs with Tesco, Rolls-Royce and Güralp Systems, in the *Tesco* and *Güralp* cases all of the individuals charged were acquitted, and the SFO ultimately dropped its investigation into the Rolls-Royce executives, (despite a DPA with a fine of £497 million).

Regulators and enforcement agencies will also want to see that the company has identified and remediated any root causes of the misconduct, including any systems and controls and cultural issues at the company. Credit is often given to those companies who take these steps proactively and at an early stage.

Finally, the extent to which a company is seen to have co-operated in the investigation is often a key determiner of the basis and terms of the settlement. In recent years, there has been much debate about the steps a company needs to take to be considered to have 'co-operated'. Some regulators and enforcement agencies have provided greater clarity and guidance in respect of what they

11 See Memorandum from Deputy Attorney General Lisa O Monaco, Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies (28 Oct. 2021), https://www.justice.gov/dag/page/file/1445106/download.

12 Strengthening the alignment of risk and reward: new remuneration rules (Jun. 2015), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2015/ps1215. Financial Conduct Authority, General guidance on the application of ex-post risk adjustment to variable compensation (1 Jul. 2015), https://www.fca.org.uk/publication/finalised-guidance/guidance-on-ex-post-risk-adjustment-variable-remuneration.pdf.

© Law Business Research 2021

consider constitutes co-operation.[13] However, some uncertainty remains about what it really means to be 'co-operative', and there are differences in expectations across jurisdictions among agencies, making it important for companies to balance these expectations when co-ordinating a global investigation and settlement.

27.7 Conclusion

The complexity of global settlements and the resultant collateral consequences in recent years means that early detection of a potential issue, through a robust compliance programme, has become all the more important. Effective and timely co-ordination of all aspects of the investigation, engagement with the different regulators involved, and consideration of the potential consequences and how to mitigate these, will be key factors in shaping the company's strategy for dealing with the matter. Identifying these issues and setting the strategy early on in the investigation is often key to ensuring that the sequencing and timing of a global settlement is ultimately achievable.

13 See, e.g., the Department of Justice policies – https://www.justice.gov/criminal-fraud/file/838416/download; and in 2021, Deputy Attorney General Monaco's memorandum, https://www.justice.gov/dag/page/file/1445106/download – and the SFO's Corporate Cooperation Guidance, https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook. In the FCA's final notice against Tesco, it referred to 'exemplary' co-operation, which included proactively offering information, constructively responding to requests and disclosing material voluntarily and agreeing not to interview witnesses without reference to the FCA (https://www.fca.org.uk/publication/final-notices/tesco-2017.pdf).

© Law Business Research 2021

28

Extraterritoriality: The UK Perspective

Anupreet Amole, Aisling O'Sullivan and Francesca Cassidy-Taylor[1]

Overview 28.1

English criminal law applies to all persons within the territory of England and Wales. However, the UK authorities can also investigate and prosecute offences committed overseas.

In the context of economic crime, the past three decades saw a sustained legislative policy of extending the jurisdiction of the UK authorities. For certain economic crimes, authorities may bring prosecutions in the United Kingdom notwithstanding that all the relevant criminal conduct occurred overseas. The most obvious example is the Bribery Act 2010 (UKBA). In line with the UK's extension of its jurisdictional reach, the authorities have increased their coordination and co-operation with other countries' prosecutors. The trend towards greater cross-border information sharing and coordinated investigations is likely to continue in accordance with ongoing domestic and international obligations.[2]

Until recently, the UK courts had endorsed the trend of cross-border criminal investigations. In the *KBR* case, the UK Serious Fraud Office (SFO) had sought to compel (under section 2(3) of the Criminal Justice Act 1987) KBR, Inc, an American company, to produce documents that it held outside the United Kingdom. This occurred as part of the SFO's investigation of certain UK subsidiaries of KBR, Inc. In 2019, the High Court held that a

1 Anupreet Amole is a partner, Aisling O'Sullivan is an associate, and Francesca Cassidy-Taylor is a chartered legal executive, at Brown Rudnick LLP. The authors thank Chloë Kealey of the firm for her assistance with this chapter.

2 For example, the Common Reporting Standard (formally the Standard for Automatic Exchange of Financial Account Information) is an initiative by the Organisation for Economic Co-operation and Development aimed at hindering tax evasion and money laundering.

© Law Business Research 2021

section 2 information notice by the SFO could have extraterritorial effect where a 'sufficient connection' exists between an overseas company and England and Wales. In particular, the Court observed that SFO investigations should not be 'frustrated or stymied' on the basis that evidence may be held on computer systems located outside the jurisdiction.

In February 2021, however, the UK Supreme Court unanimously upheld KBR's appeal, ruling that Parliament could not have intended for the SFO to use its section 2 powers extraterritorially. The Supreme Court also dismissed the notion that a 'sufficient connection' test could be implied into the Criminal Justice Act 1987.

This decision was regarded as a blow, not only to the SFO but also other UK law enforcement agencies who investigate and prosecute complex cross-border crime and have similar document production powers. The Supreme Court has made clear that those agencies cannot simply circumvent the existing mutual legal assistance (MLA) framework in relation to the taking and receiving of evidence held abroad, no matter how lengthy and cumbersome that process may be for the prosecutor.

This chapter provides an overview of the extraterritorial aspects of UK law regarding economic crime and explores how the legislative landscape is developing in an effort to keep pace with economic crime investigation and enforcement in the digital age.

28.2 The Bribery Act 2010

The UKBA created offences of (1) offering, promising or giving a bribe and (2) requesting, agreeing to receive or accepting a bribe either in the United Kingdom or abroad, in the public or private sectors, more specifically:

- sections 1 and 2 – bribing another person (active bribery) and being bribed (passive bribery);
- section 6 – bribery of a foreign public official; and
- section 7 – failure of commercial organisations to prevent bribery.

Each of the above offences has extraterritorial application, as outlined below.

28.2.1 Offences under sections 1, 2 and 6

UK prosecutors may pursue an offence under sections 1, 2 or 6, even where no part of the relevant conduct took place in the United Kingdom. This is the position provided that:

- a person's acts or omissions outside the United Kingdom would form part of such an offence if they had occurred in the United Kingdom;[3] and
- the person has a 'close connection with the United Kingdom'.[4]

3 UK Bribery Act 2010 (UKBA), s.12(2)(b).

4 ibid., s.12(2)(c).

© Law Business Research 2021

A 'close connection with the United Kingdom' is defined in the UKBA and includes British citizens and UK companies.[5]

Corporate offence under section 7 28.2.2

This offence is committed by a 'relevant commercial organisation' if a person associated with the organisation (an associated person)[6] bribes another person intending to obtain or retain business, or an advantage in the conduct of business, for the organisation. In those circumstances, the organisation's only defence to the strict liability offence is to show that it had 'adequate procedures' in place designed to prevent bribery on its behalf.[7]

A 'relevant commercial organisation' includes a company or partnership (wherever incorporated) that carries on any part of its business in the United Kingdom. On the basis of information in the public domain currently, the courts are yet to consider a case where it is disputed that a commercial organisation indicted under section 7 was carrying on business within the United Kingdom.[8] Until the courts hear argument on that specific point, practitioners continue to refer to the Ministry of Justice guidance regarding the corporate offence. That guidance recommends a 'common sense approach' and notes that a 'demonstrable business presence' is required. Neither having the company's shares listed on the London Stock Exchange nor having a UK subsidiary would necessarily mean that a foreign company is carrying on business for the purposes of section 7 of the UKBA.[9]

---

5 ibid., s.12(4). A person has a close connection with the United Kingdom if, and only if, the person was one of the following at the time the acts or omissions concerned were done or made: a body incorporated under the law of any part of the United Kingdom, a British overseas territories citizen, a British national overseas, a British overseas citizen, a person who under the British Nationality Act 1981 is a British subject, a British protected person under the British Nationality Act 1981, an individual ordinarily resident in the United Kingdom, or a Scottish partnership.

6 An 'associated person' is defined in the UKBA as a person who performs services for or on behalf of the company in any capacity (i.e., an employee, agent or subsidiary), which is to be determined by reference to all the relevant circumstances and not merely the nature of his or her relationship with the company. It is worth bearing in mind that a section 7 offence will be committed only if the associated person intended to obtain or retain business or an advantage in the conduct of business for the relevant organisation.

7 UKBA, s.7. Although 'adequate procedures' is not defined in the UKBA, the Ministry of Justice's guidance (March 2011) broadly outlines what businesses need to demonstrate to mount a successful 'adequate procedures' defence, for example proper risk-assessment procedures, due-diligence protocols and top-level commitment.

8 The section 7 offence is in addition to, and does not displace, liability that might arise under the UKBA where the commercial organisation itself commits an offence by virtue of the common law 'identification' principle. For more information on the common law 'identification principle' see the Introduction of this book.

9 Ministry of Justice Guidance to the Bribery Act 2010 (March 2011), paras. 34 to 36.

© Law Business Research 2021

It is irrelevant whether the acts or omissions forming part of the section 7 offence took place in the United Kingdom or elsewhere.[10] Therefore, it is possible for either of the following scenarios to form the factual basis for a section 7 offence:

- any business formed or incorporated in the United Kingdom, where the bribery is conducted entirely outside the United Kingdom by an associated person who has no connection with the United Kingdom and who is performing services outside the United Kingdom; and
- any business formed or incorporated outside the United Kingdom, but that carries on part of its business in the United Kingdom, where the bribery is conducted entirely outside the United Kingdom by an associated person who has no connection with the United Kingdom and who is performing services outside the United Kingdom.

In January 2020, the SFO agreed a record-breaking deferred prosecution agreement (DPA) with Airbus SE. The DPA charges Airbus with five counts of the failure to prevent offence across five jurisdictions.[11] The DPA will be in force until 31 January 2023 and is thought to be the first co-ordinated settlement agreement between the UK, US and French authorities. It is also the world's largest resolution for bribery, amounting to a total penalty of almost €3.6 billion, €991 million of which was to be paid to the SFO as disgorgement of profits, a fine and the SFO's legal and investigative costs.[12]

When advising companies on self-reporting to the authorities, practitioners should be aware of the practical risks to confidentiality. Bringing material located abroad into England and Wales may lead to legal arguments relating to its collateral use in subsequent civil or regulatory proceedings, as in *Omers Administration Corporation and others v. Tesco Plc*.[13] While that case related to documents held in England, the High Court ordered that documents provided to Tesco by the SFO during negotiations for a DPA should be disclosed by the company in a separate and subsequent civil action, brought by its shareholders.

See Chapter 3 on self-reporting to authorities

10 UKBA, s.12(5).

11 Ghana, Indonesia, Malaysia, Sri Lanka and Taiwan.

12 Other recent instances in which a company accepted charges of failure to prevent bribery, contrary to section 7, were seen in October 2020, when the SFO agreed a DPA with Airline Services Limited (ASL) under which ASL was required to pay almost £3 million and to co-operate with the SFO; and July 2021 when the SFO secured DPAs with two companies (not identified for legal reasons) under which the companies were required to pay just over £2.5 million. The July 2021 DPAs shared a common statement of facts and also covered charges of bribery contrary to s.1 UKBA.

13 [2019] EWHC 109 (Ch).

© Law Business Research 2021

The Proceeds of Crime Act 2002 28.3

Money laundering offences under Part 7 28.3.1

Money laundering has a broad meaning under UK law. The money laundering regime is designed to tackle the routes through which the proceeds of criminal activity are handled. The principal offences are found in sections 327 to 329 of the Proceeds of Crime Act 2002 (POCA), being:

- concealing, disguising, converting, transferring or removing from the United Kingdom, any criminal property (section 327);
- entering or becoming concerned in arrangements that one knows or suspects facilitate the acquisition, use, etc., of criminal property (section 328); and
- acquiring, using or possessing criminal property (section 329).

Property is 'criminal property' if it represents a person's benefit from criminal conduct; in turn, 'criminal conduct' is conduct that either is an offence in the United Kingdom or would be an offence if it had taken place within the United Kingdom.[14] Although the prosecution must adduce evidence of a predicate offence from which the proceeds of crime emanate, a prosecutor need not prove the type of predicate offence in every instance. Instead, the prosecutor will need to provide the court with detailed particulars explaining why the property should be regarded as criminal in origin, and that evidence should be sufficiently potent to demonstrate that the only reasonable inference is that the property arose from criminality.

The location of the underlying criminal conduct is immaterial. Instead, the pertinent issue is whether the conduct would constitute a criminal offence in the United Kingdom had it occurred here. This principle was confirmed by the Court of Appeal in 2014 in the case of *R v. Rogers*,[15] which served to emphasise the wide scope of the money laundering regime. Mr Rogers, a UK citizen resident in Spain, permitted money generated by a fraudulent scheme in the United Kingdom to be paid into a Spanish bank account that he controlled, and allowed another person, the scheme's principal, to withdraw money from that account. Mr Rogers was convicted under section 327(1)(c) of POCA of converting criminal property. He subsequently appealed against that conviction, arguing that the court did not have jurisdiction to hear Part 7 offences against a non-UK resident where the relevant conduct occurred entirely outside the United Kingdom.

In dismissing the appeal, the court expressly considered the wording of section 340(11)(d) of POCA, that money laundering is an act that would constitute an offence under section 327, 328 or 329 if done in the United Kingdom, and concluded that the language clearly indicated that Parliament

14 Proceeds of Crime Act 2002 (POCA 2002), s.340(2) and (3).

15 [2014] EWCA Crim 1680. This case was applied in *Jedinak v. Czech Republic* [2016] EWHC 3525 (Admin) and *Balaz v. Slovakia* [2021] EWHC 1862 (Admin) and followed in *Sulaiman v. France* [2016] EWHC 2868 (Admin).

© Law Business Research 2021

had intended for the Part 7 offences to be extraterritorial in effect. The court went on to state that, even if they were wrong on that interpretation of the statute, the modern approach to jurisdiction required 'an adjustment to the circumstances of international criminality', and noted: 'The offence of money laundering is *par excellence* an offence that is no respecter of national boundaries. It would be surprising indeed if Parliament had not intended the Act to have extra-territorial effect (as we have found it did).'[16]

In light of this extraterritorial effect, the court was able to establish a sufficient jurisdictional nexus to try Mr Rogers on the basis that the acts that led to the property becoming criminal property for the purposes of POCA plainly took place, and had an impact on victims, in the United Kingdom, and that the laundering of the proceeds by Mr Rogers in Spain was directly linked to those acts in the United Kingdom. The court added that this was:

> *not a case where the conversion of criminal property relates to the mechanics of a fraud which took place in Spain and which impacted upon Spanish victims. In those circumstances our courts would not claim jurisdiction. But in this case when the significant part of the criminality underlying the case took place in England, including the continued deprivation of the victims of their monies, there is no reasonable basis for withholding jurisdiction*[17]

Rogers and subsequent cases indicate that a person may be guilty of a money laundering offence under sections 327 to 329 of POCA in circumstances where both the predicate offending (i.e., the criminality that gives rise to the existence of proceeds of crime) and the laundering of the criminal property take place outside the territory of the United Kingdom.[18]

16 *R v. Rogers (Bradley) and others* [2014] EWCA Crim 1680 (*per* Treacy LJ) at p. 1026, paras. 52 and 54.

17 ibid. (*per* Treacy LJ) at pp. 1026 to 1027, para. 55.

18 *Sulaiman v. Tribunal de Grande Instance* [2016] EWHC 2868 (Admin) in which Dingemans J confirmed that *Rogers* is binding authority 'for the proposition that offences of money laundering extend to extraterritorial actions' (at para. 18), *Jedinak v. District Court in Pardubice* [2016] EWHC 3525 and *Balaz v. District Court of Zvolen* [2021] EWHC 1862 (Admin) in which it was 'conceded that [*Rogers*] was of general application to any offence under the money laundering provisions'. The implication of these decisions is that, while *Rogers* suggests that cases where both the predicate offence and the money laundering offence take place overseas might be decided differently, in fact in cases decided subsequent to *Rogers* this has not been the case. In *Jedinak*, despite the arguments by the defence that 'the court was clearly to an extent motivated by the recognition that some part of the offending [in *Rogers*] (and indeed the damage cause by the offending) impacted on this country and nationals of this country', the court held that 'it is clear in my judgment that the decision relating to the possible extra-territorial effect of the money laundering offences was independent of that'.

© Law Business Research 2021

There exists a limited exception described as the 'overseas conduct defence'. A person will not be liable under sections 327 to 329 if:

- he or she knew or reasonably believed that the relevant criminal conduct occurred abroad; and
- that relevant criminal conduct was not, when it took place, unlawful under the criminal law of that other country.[19]

The 'overseas conduct defence', however, does not apply to conduct that (despite being legal under local law) would constitute an offence punishable by a maximum sentence of over 12 months in the United Kingdom if it had occurred there.[20] In practice, therefore, most cases (e.g., bribery, corporate fraud, tax evasion) relevant to readers will remain squarely within the wide extraterritorial scope of POCA.

Civil recovery orders under Part 5 28.3.2

Separately, the civil recovery regime set out in POCA[21] enables UK prosecutors to seek orders from the High Court to recover property that either is or represents property obtained through unlawful conduct. As applications for civil recovery orders and property freezing orders are determined through civil, not criminal, proceedings before the High Court, the standard of proof is the balance of probabilities. The High Court may issue such an order against any person or property wherever domiciled or situated, if there is or has been a connection between the facts of the case and any part of the United Kingdom.[22] Combined with the wide jurisdictional scope of the definition of 'unlawful conduct',[23] civil recovery orders are a powerful and attractive tool in the hands of UK prosecutors.

19 POCA 2002, ss.327(2A), 328(3) and 329(2A).

20 The Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006.

21 POCA 2002, Part 5.

22 ibid., s.282A, inserted by Crime and Courts Act 2013, s.48 following the UK Supreme Court decision in *Perry v. SOCA* [2012] UKSC 35. POCA 2002, s.282A and Schedule 7A have retrospective effect – see POCA, Schedule 7A, para. 7(7).

23 Defined as (1) conduct within the United Kingdom that is unlawful under UK criminal law or (2) conduct outside the United Kingdom that is unlawful in that other country and would have been unlawful in the United Kingdom, had it occurred here. This is, therefore, a dual criminality test. The insertion in POCA 2022 of a new s.241A (by s.13 of the Criminal Finances Act 2017) adds 'gross human rights abuse or violation' to the definition of unlawful conduct for the purposes of POCA, Part 5 (civil recovery). This was the first time the United Kingdom targeted assets held anywhere in the world owned by those involved in repressive regimes; this follows the approach in the United States to a statute known as the Magnitsky Act of 2012. See Section 28.5.

© Law Business Research 2021

An additional civil recovery power became available to UK prosecutors in late January 2018.[24] On application to the High Court, prosecutors[25] can seek an unexplained wealth order (UWO) against any persons (whether or not UK domiciled) regarding their property, irrespective of that property's location. In summary, a UWO is available where:

- there is reasonable cause to believe the respondent holds specific property valued at or above £50,000;
- there are reasonable grounds to suspect that the respondent's known income is insufficient to acquire that property; and
- either the respondent is a 'politically exposed person' or there is reasonable suspicion that the respondent (or a person connected to him or her) is or has been involved in serious crime in the United Kingdom or abroad.

Where granted, the UWO compels the respondent to explain the nature of their interest in the property, and to explain how they obtained it. Failure to do so creates a presumption that the property was obtained unlawfully, and it is therefore a valid target for civil recovery proceedings under Part 5 of POCA.

The respondent, namely the person who holds or obtains the relevant property, 'includes any body corporate, whether incorporated or formed under the law of a part of the United Kingdom or in a country or territory outside the United Kingdom'.[26] By express cross-reference to section 414 of POCA,[27] it is clear that 'property is all property wherever situated'.

Where a UWO is granted against property outside the United Kingdom, and the UK prosecutor believes there is a risk of dissipation or frustration by concealing the relevant assets, that prosecutor may make a formal request for assistance from the other country's government.[28] Since their introduction in early 2018, and at the time of writing, the National Crime Agency (NCA) has secured UWOs in four separate cases.[29]

See Chapter 30 on individual penalties

In June 2020, however, the NCA encountered its first setback when the Court of Appeal ruled that it had 'no real prospect' of succeeding in overturning the High Court's decision in April 2020 in *NCA v. Baker and Others*,[30] which ordered the

24 See Criminal Finances Act 2017, Part 1, which amends POCA.

25 Under POCA, s. 362A(7), enforcement agencies permitted to apply for a UWO include the National Crime Agency, the Serious Fraud Office, HM Revenue and Customs, the Financial Conduct Authority and the Director of Public Prosecutions.

26 POCA, s.362H(5), inserted by Criminal Finances Act 2017, s.1.

27 ibid., s.362H(6), inserted by Criminal Finances Act 2017, s.1.

28 ibid., s.362S, inserted by Criminal Finances Act 2017, s.3.

29 At the time of writing, the NCA has successfully defended two UWOs: *National Crime Agency v. Hajiyeva* [2020] EWCA Civ 108; and *National Crime Agency v. Mansoor Hussain* and others [2020] EWHC 432 (Admin).

30 [2020] EWHC 822 (Admin). The NCA sought orders to compel four offshore companies to explain the source of funds used to buy five London homes for £80 million which, it claims, were purchased using illicit funds generated by Mr Aliyev's late father.

© Law Business Research 2021

discharge of three UWOs obtained by the NCA against Nurali Aliyev, the grandson of former Kazakh president, Nursultan Nazarbayev. In its ruling,[31] the Court of Appeal found that the case presented by the NCA was 'flawed by inadequate investigation into some obvious lines of enquiry'.[32] The decision is an instructive example of the court's approach to robust scrutiny of UWO applications.

Tax evasion and the Criminal Finances Act 2017 28.4

The Criminal Finances Act 2017 also introduced a new corporate offence focused on tax evasion. As with the UKBA's corporate offence, this represents another significant departure from the traditional 'directing mind' identification doctrine for corporate criminal liability under English law.

See Chapter 1

Part 3 of the Criminal Finances Act 2017 creates two corporate offences of failure to prevent the facilitation of tax evasion. The offences are modelled on section 7 of the UKBA and apply to both domestic and overseas tax evasion. The offences are (1) failure to prevent the facilitation of UK tax evasion offences (section 45) and (2) failure to prevent the facilitation of foreign tax evasion offences (section 46).

If the offence took place outside the jurisdiction, however, UK prosecutors must still prove to the criminal standard that both the taxpayer and the associated person committed an offence. The prosecutor will also need to prove dual criminality of the conduct. The offences consist of three component parts. First, the prosecution must prove criminal evasion by a taxpayer; and there must have been dishonest[33] facilitation of tax evasion by an associated person.[34] Where these two components are satisfied, the relevant body is criminally liable (unless it can show that it had 'reasonable preventative procedures' in place, or that it was unreasonable to expect the company to have had such procedures in place).

A 'relevant body' is a company or a partnership, wherever it may be incorporated or formed.[35] A 'person associated' with the relevant body is an

31 Order available at: https://globalinvestigationsreview.com/digital_assets/5177505d-8751-4434-a19e-6d931ac70bf0/Court-of-Appeal-%5b1%5d.pdf.

32 ibid.

33 The test for dishonesty must now be viewed in light of the Supreme Court's decision in *Ivey v. Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67, which disapproved the second limb of the well-known test in *R v. Ghosh* [1982] EWCA Crim 2. Although the observations of the court were technically *obiter*, the Court of Appeal (Criminal Division) has indicated that *Ivey* correctly reflects the law – see *R v. Pabon* [2018] EWCA Crim 420. The test in *Ivey* was affirmed in *Barton and Booth v. R* [2020] EWCA Crim 575.

34 The ruling of the Court of Appeal in *Barton and Booth v. R* [2020] EWCA Crim 575 in April 2020, in endorsing *Ivey*, affirmed that the test for dishonesty should be judged by reference to society's standards rather than the defendant's understanding of those standards. The ruling renders organisations and their senior executives or employees more vulnerable to conviction when charged in cases involving fraud and other dishonesty-related offences.

35 Criminal Finances Act 2017, s.46(2).

© Law Business Research 2021

employee, an agent or any other person performing services for or on behalf of that relevant body.[36] Again, this is broadly comparable to the concepts in the UKBA. Section 46 of the Criminal Finances Act 2017 provides that a company or partnership that carries on business in the United Kingdom will commit an offence if a 'person associated' with it commits a 'foreign tax evasion facilitation offence', unless the company or partnership had reasonable procedures in place to prevent the facilitation offence. A foreign tax evasion facilitation offence means conduct that:

> *amounts to an offence under the law of a foreign country, . . . relates to the commission by another person of a foreign tax evasion offence under the law of that country, and . . . would, if the foreign tax evasion offence were a UK tax evasion offence, amount to a UK tax evasion facilitation offence*[37]

28.5 Financial sanctions

Financial sanctions restrict the provision of financial services, or access to global capital markets, or both. More specifically, those restrictions can include bans on investments in a particular country, or the denial of banking relationships. Trade sanctions restrict the trading of certain products or commodities (e.g., arms, oil and diamonds) from targeted countries (e.g., Iran, Russia and Syria) and control the export of certain products (e.g., military or dual-use items) to targeted countries.[38]

For the purposes of this chapter, we focus on financial sanctions.[39] On 1 January 2021, the United Kingdom's legal framework regarding financial sanctions was consolidated under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). Previously, the United Kingdom used secondary legislation to implement various sanctions programmes made by the United Nations Security Council and the European Union. This post-Brexit sanctions

36 ibid., s.44(4).

37 ibid., s.46(6).

38 A decision by the European Court of Justice, which upheld the EU sanctions against Russia regarding its annexation of Crimea in 2014, demonstrates the rationale in practice. See *PJSC Rosneft Oil Company v. Her Majesty's Treasury and Others*, Case C-72/15, 28 March 2017.

39 For trade sanctions, see the Export Control Act 2002 (and the related Export Control Order 2008) and the Customs and Excise Management Act 1979. The Customs and Excise Management Act 1979 imposes criminal liability where a person exports goods from the United Kingdom 'when the exportation or shipment is or would be contrary to any prohibition or restriction for the time being in force'. The Export Control Order (ECO) 2008 imposes those restrictions. The ECO 2008 specifies a three-tier categorisation of goods, with Category A products including items designed for torture, Category B including arms and ammunition, and Category C being items that have a dual civil/military use. See Part 4 and Schedule 1 of the ECO 2008. Trade sanctions apply to (1) anybody present in the United Kingdom, i.e., all persons (natural and legal), (2) all UK subjects anywhere in the world, and (3) any legal entity incorporated under UK law.

© Law Business Research 2021

framework has given the United Kingdom a new and broad discretion to amend and update its domestic regime. The UK Foreign, Commonwealth and Development Office has implemented a number of regulations to replace the EU sanctions regimes (as implemented in the United Kingdom) with domestic regulations. The United Kingdom has also adopted country-specific regulations to replace the equivalent EU regulations that restrict activities in respect of certain countries or territories as well as certain terrorist organisations.[40]

In July 2020, the British government announced the UK Global Human Rights Sanctions Regulations 2020 (the Regulations),[41] pursuant to SAMLA.

The Regulations empower the Foreign Secretary to designate persons (whether or not UK persons) according to specific criteria and impose asset freezes and travel bans.[42]

In April 2021, the United Kingdom enacted the Global Anti-Corruption Sanctions Regulations 2021 specifically targeting individuals suspected of involvement in serious corruption.[43] The new regime is designed to complement the Regulations. The scope of the regime is wide and allows for an individual or entity to be designated if there are reasonable grounds to suspect that the person is involved in serious corruption. Indirect involvement through, for example, an entity owned or controlled directly or indirectly by a person who is or has been so involved, is also captured.[44] As with the 2020 Regulations, the new regime operates through specific asset freezes and travel bans on individuals and entities.[45]

---

40 A number of regulations have been enacted under SAMLA that mirror sanctions measures previously in force in the United Kingdom under EU Regulations. Those enactments merely give the new measures an independent statutory footing under UK law.

41 https://www.legislation.gov.uk/uksi/2020/680/made. The accompanying statutory guidance is available at https://www.gov.uk/government/publications/global-human-rights-sanctions-guidance/global-human-rights-sanctions-guidance.

42 The designation criteria in Regulation 6(3) are broadly defined and include anyone who 'is responsible for or engages in' human rights abuses; 'facilitates, incites, promotes or provides support for such an activity'; 'provides financial services, or makes available funds, economic resources, goods or technology, knowing or having reasonable cause to suspect that those financial services, funds, economic resources, goods or technology will or may contribute to such an activity'; 'provides financial services, or makes available funds, economic resources, goods or technology to a person [responsible for or engaged in human rights abuse]'; who 'profits financially or obtains any other benefit from an activity' violating human rights.

43 https://www.legislation.gov.uk/uksi/2021/488/contents/made.

44 The Regulations define involvement in serious corruption widely. Corruption, however, includes bribery and the misappropriation of property. As such, the Regulations revoke the UK's specific misappropriation related-sanctions regulations.

45 As of August 2021, there have been 27 individual designations under the Regulations. The accompanying statutory guidance is available at https://www.gov.uk/government/publications/global-anti-corruption-sanctions-guidance.

© Law Business Research 2021

The United Kingdom may also issue financial sanctions under certain specific statutes, such as the Terrorist Asset-Freezing Act 2010.[46] The specific restrictions imposed by any one set of financial sanctions (e.g., those relating to Russia's involvement in Ukraine) will vary in each case. Those advising businesses concerned about liability should carefully review the text of the specific statutory instrument, and the underlying EU regulation, in each case. Broadly, however, UK financial sanctions impose criminal liability for a person who:

- makes funds or economic resources available, whether directly or indirectly, to a designated person;
- deals with funds or economic resources belonging to or controlled by a designated person; or
- acts in a way, whether directly or indirectly, to circumvent the relevant financial sanction prohibitions.[47]

While the jurisdictional scope of UK financial sanctions is broad, they do require some element of UK nexus. The sanctions apply to:

- anybody present in the United Kingdom, namely all persons (natural and legal) 'who are within or undertake activities within the UK's territory'; and
- all UK nationals and all UK legal entities (including branches, and the UK subsidiaries of foreign companies), wherever they may be in the world and irrespective of where their activities occur.[48]

In its updated guidance, the Office of Financial Sanctions Implementation (OFSI) states that a sanctions breach need not occur within UK borders for its authority to be engaged, but that any such breach must have a 'UK nexus', which OFSI will determine on the facts of each case.[49] This may provide some degree of comfort to foreign businesses with no UK footprint. Notably, SAMLA provides for sanctions being imposed regarding (1) conduct within UK jurisdiction by any person and (2) conduct anywhere in the world but only if the conduct is by a 'United Kingdom person'.[50]

The Policing and Crime Act 2017 introduced a wider range of enforcement options, specifically (1) making sanctions offences eligible for consideration

46 The other relevant UK statutes, which also take a broad jurisdictional approach, are the Counter-Terrorism Act 2008 and the Anti-terrorism, Crime and Security Act 2001.

47 Office of Financial Sanctions Implementation (OFSI), Financial Sanctions: Guidance, March 2018, p. 12. The maximum term of imprisonment was recently increased from two to seven years – see Policing and Crime Act 2017 (PCA 2017), ss.144 and 145.

48 OFSI, Financial Sanctions: Guidance, March 2018, p. 7.

49 OFSI, Monetary penalties for breaches of financial sanctions: Guidance, April 2021. The prior version of the Guidance stated (at para. 3.8) that OFSI 'will not artificially bring something within UK authority that does not naturally come under it'. This statement regarding OFSI's jurisdiction over financial sanctions breaches has been removed from the revised guidance and may signal a more expansive interpretation of OFSI's jurisdiction to impose penalties.

50 Sanctions and Anti-Money Laundering Act 2018, s.21.

© Law Business Research 2021

for a DPA,[51] (2) making sanctions offences eligible for (civil) Serious Crime Prevention Orders under the Serious Crime Act 2007[52] and (3) empowering OFSI to impose (civil) financial penalties.[53] In April 2020, OFSI utilised is powers under the Act and announced that it had imposed a £20.4 million penalty on Standard Chartered for breaches of EU 'sectoral sanctions' on Russian companies in the banking, oil and defence sectors.[54] This case is by far OFSI's largest and most significant sanctions enforcement action to date.

See Chapter 44 on sanctions

Conspiracy 28.6

Readers will be familiar with cases involving suspected or alleged conspiracies to commit substantive offences. When considering conspiracy in the economic crime context, practitioners should be aware of the interplay between (1) common law conspiracy to defraud, (2) the conspiracy offence in section 1A Criminal Law Act 1977, and (3) the Fraud Act 2006, whose extraterritorial reach is specified by the Criminal Justice Act 1993 (as amended).

Common law conspiracy to defraud 28.6.1

Common law conspiracy to defraud is one of the very few remaining common law conspiracy offences, section 5 of the Criminal Law Act 1977 having replaced all others with a general statutory offence. Statute has made clear that a person charged with conspiracy to defraud may be liable irrespective of whether he or she became a co-conspirator in England or whether any act in relation to the conspiracy occurred in England.[55]

Statutory conspiracy to commit offences abroad 28.6.2

The Criminal Justice Act 1987 provides that a prosecutor may pursue common law conspiracy to defraud even in circumstances where the substantive offence would be covered by a specific statute.[56] However, in many cases, ranging from *Innospec Limited*[57] in 2010 to the attempted prosecution of Barclays Bank

51 PCA 2017, s.150.

52 ibid., s.151.

53 ibid., s.146.

54 OFSI, HM Treasury, Report of Penalty for Breach of Financial Sanctions Regulations (section 149(2) PACA 2017 report) Imposition of Monetary Penalty – Standard Chartered Bank, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.

55 Criminal Justice Act 1993, s.3(2).

56 Criminal Justice 1987, s.12, which retained the offence at common law of conspiracy to defraud – see Criminal Law Act 1977, s.5(2).

57 The charge against Innospec Ltd was that between February 2002 and December 2006, the company, through various agents, engaged in systematic and large-scale corruption of senior government officials of Indonesia to secure contracts for the supply of a fuel additive, tetraethyl lead (TEL). The corrupt behaviour took the form of bribes, totalling approximately US$8 million. The seriousness of the corruption was aggravated by the fact

© Law Business Research 2021

regarding Qatar and the recent convictions of a number of former Unaoil executives for bribery offences in Iraq,[58] the SFO has relied on section 1(1) of the Criminal Law Act 1977 to bring charges of conspiracy to commit offences.[59]

In 1998, the Criminal Law Act 1977 was amended to provide expressly for a discrete offence of conspiracy to commit criminal offences outside the jurisdiction.[60] By section 1A of the Act, a conspiracy may involve the doing of an act in a place outside England and Wales that constitutes an offence in that other jurisdiction. The purpose of section 1A was to extend existing UK law, and to give the English courts extraterritorial jurisdiction in relation to a conspiracy (1) partly formed or carried out in England and Wales, and (2) where the object was the commission of a foreign offence (where there is an equivalent offence in England and Wales). This section only applies, however, where four nexus conditions are satisfied.[61]

Similarly, the Fraud Act 2006 has expressly broad extraterritorial application.[62] Put simply, where any element of a statutory fraud offence[63] occurs within England and Wales, the court will have jurisdiction to try a defendant whether or not he or she was in the jurisdiction at any material time, and whether or not he or she was a British citizen at the time.

---

that Innospec Ltd's behaviour was aimed at blocking legislative moves to ban TEL, owing to environmental and public health concerns. The company pleaded guilty to conspiracy contrary to Criminal Law Act 1977, s.1 and was fined US$12.7 million.

58 https://www.sfo.gov.uk/2020/07/13/former-unaoil-executives-guilty-of-giving-corrupt-payments-for-oil-contracts-in-post-occupation-iraq/, accessed 26 July 2020.

59 In *R v. Turner, Kerrison, Papachristos and Jennings* in 2014 (and the subsequent appeal *SFO v. Papachristos and Kerrison* [2014] EWCA Crim 1863), four former executives of Innospec Ltd were convicted and imprisoned for conspiracy offences in relation to their roles in bribing state officials in Indonesia and Iraq to secure contracts for the supply of products produced by Innospec Ltd.

60 Inserted by Criminal Justice (Terrorism and Conspiracy) Act 1998, s.5.

61 The conditions set out in Criminal Law Act 1977 (CLA 1977), s.1A(6) are pursuit of the agreed conduct would involve an act by one or more of the parties outside the United Kingdom; that act is an offence under local law in that other country; the agreement would be a conspiracy (within CLA 1977, s.1(1)) but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions; and a party to the agreement, whether directly or via an agent, did anything in England and Wales regarding formation of the agreement before its formation, became a party to it in England and Wales, or did or omitted anything in England and Wales pursuant to the agreement. Where those conditions are satisfied, the prosecutor may pursue conspiracy charges under s.1A, referring to the offence as being a conspiracy to commit the underlying substantive offence (e.g., drug trafficking or people smuggling) but for the fact that it was not triable in England and Wales.

62 Criminal Justice Act 1993, Part 1, as amended by the Fraud Act 2006 (Schedule 1).

63 Being fraud by false representation (Fraud Act 2006, s.2), fraud by failing to disclose information (ibid., s.3), or fraud by abuse of position (ibid., s.4).

© Law Business Research 2021

Inchoate offences 28.6.3

Separately, practitioners should not overlook the inchoate offences of encouraging or assisting others in the commission of offences. The Serious Crime Act 2007 includes statutory inchoate offences (under sections 44 to 46) of encouraging or assisting the commission of offences; these have extraterritorial application in certain circumstances.[64]

Mutual legal assistance, cross-border production and the extraterritorial authority of UK enforcement agencies 28.7

MLA allows one state to seek co-operation from another in the investigation or prosecution of criminal offences via a formal letter of request.[65]

The framework governing the United Kingdom's approach to MLA is contained in statute, primarily the Crime (International Co-operation) Act 2003 (CICA), the European Convention on Mutual Legal Assistance in Criminal Matters 2000, and various bilateral and multilateral treaties (for example, with the United States in 1994, with Brazil in 2005 and with India in 1995). The UK Home Office Central Authority[66] is primarily tasked with receiving, and acceding to, MLA requests.[67]

Outgoing MLA requests (i.e., those from the United Kingdom to a foreign state) seeking evidence must be issued by a court or a designated prosecuting authority.[68]

Evidence obtained from or by the United Kingdom pursuant to an MLA request cannot be used for any purpose other than that specified in the request without consent of the foreign authority.

---

64 Through operation of Serious Crime Act 2007, s.52, and the conditions specified in Schedule 4.

65 While MLA is used for gathering and exchanging information, and requesting and providing assistance in obtaining evidence located abroad, extradition is the legal process by which an individual is transferred from one state to another for the purposes of being tried or serving a sentence already imposed. The Extradition Act 2003 sets out the UK extradition legal framework. MLA is generally not appropriate if the material can be obtained directly via law enforcement co-operation for intelligence purposes or if the material otherwise is admissible in that form.

66 There are exceptions such as EU freezing orders for property, which need to be sent directly to the relevant UK prosecuting authority.

67 Through operation of Serious Crime Act 2007, s.52, and the conditions specified in Schedule 4. Following the end of the Brexit transition period on 31 December 2020, the provisions of the European Union's Framework Decisions 2003/577/JHA (on Mutual Recognition of Freezing Orders) and 2006/783/JHA (on Mutual Recognition of Confiscation Orders) and the replacement Regulation 2018/1805 no longer apply to the United Kingdom. Requests for assistance in relation to restraint and confiscation should be made directly to the UK Central Authority under the provisions of the UK–EU Trade and Cooperation Agreement, Part 3, Title XI.

68 The Director and any designated member of the SFO, the Financial Conduct Authority and the Bank of England are examples of designated prosecuting authorities.

© Law Business Research 2021

In practice, persons subject to a request from a foreign authority, whether formal or informal, should ensure that they do not disclose material that is legally privileged, and ensure they take all appropriate steps to protect their rights under UK law, including as to the privilege against self-incrimination. For example, one method of MLA to foreign states is to compel witnesses to attend court.[69] Importantly, however, a witness cannot be compelled to give evidence where he or she could not otherwise be compelled to testify under either UK law or that of the requesting state.[70]

Mutual legal assistance is not, of course, the only avenue for UK authorities to extend their information-gathering overseas. In February 2019, the Court of Appeal decided the case of *Jimenez*.[71] The Court held that Her Majesty's Revenue and Customs (HMRC) was entitled to serve an 'information notice'[72] on a British individual resident overseas to obtain information about his tax position. Mr Jimenez, a UK national resident in the United Arab Emirates, challenged service of that notice at his address in Dubai. HMRC had served the notice as part of its investigation into Mr Jimenez's tax affairs. In 2017, the High Court quashed the notice on the basis that Schedule 36 to the Finance Act 2008 was silent as to its extraterritorial effect. The Court of Appeal subsequently overturned that decision on the basis that the purpose of Schedule 36 is to prevent tax evasion, which is often cross-border in nature and, in the absence of any express restriction on the geographical effect, the legislation must confer effective investigatory powers on HMRC. In short, the Court of Appeal held that Parliament intended that specific information-gathering power should be available for investigating the UK tax position of relevant persons resident overseas.[73] Permission to appeal the decision was granted in June 2019, but a hearing has not yet been fixed by the Supreme Court.

See Chapter 11 on production of information to authorities

The Crime (Overseas Production Orders) Act 2019 introduced an information gathering tool for UK agencies. Since data is increasingly managed, processed and stored by entities located outside the United Kingdom, the Act

69 Crime (International Co-operation) Act 2003, s.15.

70 ibid. Schedule 1.

71 *R (on the application of Tony Michael Jimenez) v. First Tier Tax Tribunal (Tax Chamber) and HMRC* [2019] EWCA Civ 51.

72 Pursuant to Finance Act 2008, Schedule 36, para. 1.

73 The Court also dismissed Mr Jimenez's argument that HMRC's conduct amounted to an exercise of UK official acts in the territory of another sovereign state. The Court held that service of the information notice did not seek to impose any criminal liability on a foreign national, and did not offend against the territorial sovereignty of the United Arab Emirates. Interestingly, in the leading judgment given by Lord Justice Patten noted that: 'the more recent decision[s] of the Supreme Court in *Bilta* and the Divisional Court in *KBR* confirm that the jurisdiction to serve a notice requiring the provision of information from a person resident abroad or even to impose liability on the recipient will not raise eyebrows where they serve to protect a sufficient national interest. In my view, the present case falls squarely within that category of case'.

© Law Business Research 2021

enables specified investigative agencies[74] to apply to a Crown Court judge for an overseas production order (OPO). An OPO enables receipt of electronic data directly from an overseas communications service provider. The government has stated that this will be subject to robust judicial oversight, and that there are existing statutory protections for legally privileged or journalistic material.

The United Kingdom has entered into a data access agreement with the United States[75] that will enable UK law enforcement agencies to request electronic data, via warrant, from US tech companies, speeding up the investigation and prosecution of serious criminals and replacing the existing MLA regime.

Transparency of corporate ownership

Among other things, one of the primary purposes of SAMLA was to curb money laundering in British overseas territories such as the British Virgin Islands (BVI), the Cayman Islands and the Crown dependencies.[76]

While there has been momentum towards establishing publicly available registers of corporate beneficial ownership,[77] some overseas British territories resisted the change at a political level.[78] In particular, the government of Bermuda has opposed the register, arguing that the imposition of the register is an affront to the constitutional standing of Bermuda, while other territories have resisted the change on economic grounds. As a result, in December 2020, the UK government published an Order in Council[79] requiring all overseas territories to establish public registers.[80]

74 These include the SFO, the National Crime Agency, the police, HMRC and the Financial Conduct Authority.

75 Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No. 6/2019] (https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019), accessed on 21 July 2020. This Agreement is facilitated by the Crime (Overseas Production Orders) Act 2019.

76 Guernsey, the Isle of Man and Jersey.

77 For example, the Cayman Islands and Bermuda have committed to providing beneficial ownership registers by 2022.

78 For example, the government of Bermuda has opposed the register, arguing that the imposition of the register is an affront to the constitutional standing of Bermuda.

79 'The Overseas Territories (Publicly Accessible Registers of Beneficial Ownership of Companies: draft Order in Council, published 14 December 2020.

80 Some territories, such as the Cayman Islands, have reacted positively, declaring they will be compliant with a fully transparent company ownership register by 2022. Jersey, Guernsey and the Isle of Man have jointly made a similar commitment for public registers by 2023.

© Law Business Research 2021

29

Extraterritoriality: The US Perspective

James P Loonam and Ryan J Andreoli[1]

29.1 Extraterritorial reach of US laws

Investigations conducted by US prosecutors and regulators often concern conduct outside the United States and involve evidence located abroad. The two questions of whether US law applies to the conduct under investigation and whether US authorities can compel the production of evidence located abroad are of significant importance to practitioners. As to the first question, in a series of civil cases, the United States Supreme Court has reasserted a presumption against the extraterritorial application of US statutes.[2] What this means is that lower US courts have been instructed to assume that US law applies only to conduct that takes place within the borders of the United States unless the particular law explicitly states it has extraterritorial application. In practice, this presumption is an important but limited check on US prosecutors' and regulators' powers to investigate and bring cases involving foreign conduct. Even limited contacts with the United States, such as the use of the US wires or financial system, may bring related conduct that takes place outside the United States within the domestic purview of certain US laws. Courts look to the statute's 'focus'[3] to determine whether a case involves a domestic application of a statute:

1 James P Loonam and Ryan J Andreoli are partners at Jones Day. Conor Reardon, a former associate at Jones Day, made a substantial contribution to this chapter.

2 *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010); *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013); *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

3 *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010); *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

© Law Business Research 2021

> *If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in US territory.*[4]

In addition, courts have reasoned that 'the extraterritorial reach of an ancillary offense such as conspiracy is coterminous with that of the underlying statute'.[5] In recent years, lower courts have grappled with this issue of determining the focus of various statutes case by case and have not always reached consistent results. This chapter will address the recent jurisprudence in this area, focusing on statutes that are most commonly invoked to reach overseas conduct. As to the second question, US prosecutors often seek to obtain evidence located overseas during the course of investigations. This chapter will address the muscular stance taken by prosecutors to obtain evidence located overseas from non-US entities and the support this approach has found in the courts to date.[6]

Securities laws 29.2

The Securities Exchange Act of 1934 (the Exchange Act) regulates domestic securities markets and transactions. Its general anti-fraud provision, Section 10(b), along with accompanying SEC Rule 10b-5, prohibits fraud in connection with the purchase or sale of securities. The Exchange Act and its associated rules are enforced civilly by the SEC (as well as through private actions) and criminally by the US Department of Justice (DOJ). Much extra-territoriality litigation – including the Supreme Court's landmark decision in *Morrison v. Nat'l Australia Bank Ltd*[7] – has involved the securities laws.

The Morrison decision 29.2.1

Some forty years before *Morrison*, the Second Circuit developed an approach to extraterritoriality in the securities fraud context that would be adopted (albeit with variation) by many other courts of appeals.[8] Under this 'conduct and effects' test, the court determined the extraterritorial reach of the securities laws in a given case by asking (1) 'whether the wrongful conduct had a substantial effect in the United States or upon United States citizens', and (2) 'whether the wrongful conduct occurred in the United States'.[9] Other circuits adopted

4 *RJR Nabisco*, 136 S. Ct. at 2101.

5 *United States v. Napout*, 963 F.3d 163, 179 (2d Cir. 2020) (quoting *United States v. Hoskins* 902 F.3d 69, 96 (2d Cir. 2018)).

6 See, e.g., *In re: Sealed Case*, No. 19-5068 (D.C. Cir. 6 August 2019).

7 561 U.S. 247 (2010).

8 See *Leasco Data Processing Equip. Corp. v. Maxwell*, 468 F.2d 1326 (2d Cir. 1972); *Schoenbaum v. Firstbrook*, 405 F.2d 200 (2d Cir. 1968).

9 *Morrison*, 561 U.S. at 257 (quoting *SEC v. Berger*, 322 F.3d 187, 192–93 (2d Cir. 2003)).

© Law Business Research 2021

related (though not identical) tests.[10] Whatever the precise formulation, the conduct-and-effects approach required a fact-intensive, case-specific inquiry calculated to reveal whether Congress would have wanted United States law to apply had it considered the matter.[11]

In *Morrison*, the Supreme Court rejected this long-standing test. The Court criticised the notion that congressional silence on the extraterritorial scope of Section 10(b) gave judges licence to 'determine what Congress would have wanted'.[12] It added that the imprecise conduct-and-effects approach was inconsistent in application and yielded unpredictable results.[13] The proper approach, the majority held, was to apply the presumption against extraterritoriality in all cases.[14] Because Section 10(b) lacked 'a clear statement of extraterritorial effect', it applied only domestically.[15]

The Court went on to describe the domestic scope of Section 10(b). The statute's focus is not merely deceptive conduct, but deceptive conduct 'in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered'.[16] Therefore, Section 10(b) applies only to 'transactions in securities listed on domestic exchanges, and domestic transactions in other securities'.[17]

In explaining the territorial reach of Section 10(b), the Court upset existing case law in another respect. Many courts had considered a statute's extraterritorial scope to raise a question of subject-matter jurisdiction.[18] Not so, wrote the majority: to 'ask what conduct Section 10(b) reaches is to ask what conduct Section 10(b) prohibits', which is not a question of adjudicative authority but 'a merits question'.[19]

29.2.2 Post-Morrison developments

In *Morrison*, the Court announced that its new approach was (unlike the conduct-and-effects standard) a 'clear test' that could be predictably applied.[20] Nonetheless, lower courts have wrestled with a number of questions that *Morrison* did not answer.

One fundamental issue arises not from any lack of clarity in *Morrison* but from Congress's apparent response to the decision. Days after *Morrison* came down, a joint congressional committee finalising the proposed Dodd-Frank

10 See *Morrison*, at 259 (collecting cases).

11 Id. at 259–60.

12 Id. at 260.

13 Id.

14 Id.

15 Id. at 265.

16 Id. at 266–67 (quoting 15 U.S.C. § 78j(b)).

17 Id.

18 Id. at 253–54.

19 Id. at 254.

20 Id. at 269.

© Law Business Research 2021

Act published a final version of the bill, which would be enacted less than a month later.[21] That version (and the enacted law) included a provision, Section 929P, that appears calculated to abrogate *Morrison* in the context of SEC and criminal actions. It amends the jurisdictional section of the Exchange Act by providing that district courts 'shall have jurisdiction' over such actions involving 'conduct within the United States that constitutes significant steps in furtherance of the violation' or 'conduct occurring outside the United States that has a foreseeable substantial effect within the United States'.[22] The legislator who had drafted the provision, Representative Paul Kanjorski, stated that its purpose 'was to make clear that the antifraud provisions apply extraterritorially in enforcement actions'.[23]

The intent behind Section 929P seems clear enough, but *Morrison* explicitly held that the question of a statute's extraterritorial application is a merits question, not a jurisdictional question. Section 929P speaks only to jurisdiction and leaves untouched the substantive anti-fraud provisions of the Exchange Act. Faced with this conflict between contextual evidence of congressional intent and plain text, several courts have sidestepped the issue.[24] But in 2019, the Tenth Circuit became the first court of appeals to directly confront the question. The court prioritised 'context and historical background' – particularly Congress's inability to respond to *Morrison*'s jurisdiction/merits holding in the days between the decision and reporting of the final bill – to hold that Section 929P abrogated *Morrison* and that 'the substantive antifraud provisions should apply extraterritorially when the statutory conduct-and-effects test is satisfied'.[25] In May 2021 the First Circuit followed suit.[26] Whether other courts of appeals will embrace the Tenth Circuit's conclusion remains to be seen.[27]

In addition to this basic question of *Morrison*'s vitality outside the context of private actions, courts have addressed a number of issues regarding its

21 Pub. L. No. 111-203, 124 Stat. 1376 (2010).

22 15 U.S.C. § 78aa(b).

23 *SEC v. Scoville*, 913 F.3d 1204, 1218 (10th Cir. 2019), cert. denied, 18-1566 (4 November 2019).

24 See, e.g., *SEC v. Chicago Convention Ctr., LLC*, 961 F. Supp. 2d 905, 911–17 (N.D. Ill. 2013) ('The plain language of Section 929P(b) and its placement in the jurisdictional section of the Exchange Act indicate that it may be jurisdictional. It is unclear, however, whether the Court's analysis should stop there because it is possible that this interpretation would create superfluity or contradict the legislative intent. The Court need not resolve this complex interpretation issue, however, because . . . under either the Morrison "transactional" inquiry or the allegedly revived "conduct and effects test," the SEC's Complaint survives the present motion to dismiss.').

25 *Scoville*, 913 F.3d at 1218.

26 *SEC v. Morrone*, 997 F.3d 52, 60 n.7 (1st Cir. 2021) ('We note that *Morrison*'s transactional test only governs conduct occurring before July 22, 2010. Shortly after *Morrison* was decided, Congress amended the federal securities laws to "apply extraterritorially when the [newly added] statutory conduct-and-effects test is satisfied".')

27 At least one district court outside the Tenth Circuit has also followed *Scoville*. See *SEC v. Montano*, 2020 WL 5534653 *7 (M.D. Fla. 24 Jul. 2020).

© Law Business Research 2021

application. The first prong of *Morrison*'s transactional test permits actions based on 'transactions in securities *listed* on domestic exchanges'.[28] In 2014, the Second Circuit considered whether this formulation permitted a 'foreign-cubed' claim – foreign institutional investors suing foreign banking defendants over shares purchased on a foreign exchange – because those shares were cross-listed on the New York Stock Exchange.[29] The court acknowledged that the plaintiffs' 'listing theory' comported with *Morrison*'s language 'taken in isolation', but concluded that, 'read as a whole', *Morrison* made clear that domestic application of the Exchange Act requires that the shares in question be purchased, not just listed, on a domestic exchange.[30] Courts have also addressed just what qualifies as a domestic exchange. One district court held in 2011 that *Morrison*'s first prong reaches securities traded on domestic over-the-counter markets, reasoning that 'transactions on the domestic over-the-counter market are as imbued with our national interest as trades on national exchanges'.[31] But that decision appears to be an outlier. Other courts have concluded that over-the-counter transactions may qualify under *Morrison*'s second prong (as domestic transactions in other securities), but do not occur on exchanges.[32]

Morrison's second prong has likewise received attention from litigants and courts. In 2012, the Second Circuit held that a securities transaction is domestic under *Morrison* if (1) 'the purchaser incurred irrevocable liability within the United States to take and pay for a security', (2) 'the seller incurred irrevocable liability within the United States to deliver a security' or (3) 'title to the shares was passed within the United States'.[33] Under the 'irrevocable liability' test, the court must identify 'the point at which the parties obligated themselves to perform what they had agreed to perform even if the formal performance of their agreement is to be after a lapse of time'.[34] What matters is not where the 'contract is said to have been executed' as a matter of contract law, but 'where, physically, the purchaser or seller committed him or herself'.[35] The Second

28 *Morrison*, 561 U.S. at 267 (emphasis added).

29 *City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG*, 752 F.3d 173, 179–80 (2d Cir. 2014).

30 Id. at 180–81.

31 *SEC v. Ficeto*, 839 F. Supp. 2d 1101, 1108 (C.D. Cal. 2011); see id. at 1108–14; see also *Rubenstein v. Cosmos Holdings Inc.*, 2020 WL 3893347 *11 (S.D.N.Y. 10 Jul. 2020) (assuming that transactions involving a corporation listed on the OTCQB market satisfied *Morrison*'s transactional test while acknowledging the contrary holding of *Stoyas).*

32 See, e.g., *Stoyas v. Toshiba Corp.*, 896 F.3d 933, 945–47 (9th Cir. 2018); *United States v. Georgiou*, 777 F.3d 125, 134–35 (3d Cir. 2015); *In re Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Prods. Liab. Litig.*, Nos. 15-cv-6167, 15-cv-6168, 16-cv-190, 16-cv-184, 2017 WL 66281, at *3–4 (N.D. Cal. 4 Jan. 2017); *Acerra v. Trulieve Cannabis Corp.*, No. 4:20-cv-186-RH-MJF, 2021 WL 1269919, at *4 (N.D. Fla. 18 Mar. 2021).

33 *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 68–69 (2d Cir. 2012).

34 Id. at 68.

35 *United States v. Vilar*, 729 F.3d 62, 77 n.11 (2d Cir. 2013). Notwithstanding this focus on where, 'physically', the parties committed themselves, the Second Circuit has also stated that

© Law Business Research 2021

Circuit's approach has met generally with approval and has been expressly adopted by the First, Third and Ninth Circuits.[36] Determining whether irrevocable liability was incurred, or title passed, in the United States requires analysis of 'factual allegations concerning contract formation, placement of purchase orders, passing of title, and the exchange of money'.[37] Given the varied and complex nature of modern transactions in securities, the moment of irrevocable commitment (or passing of title) will not always be obvious.[38]

Finally, there is disagreement among several of the circuit courts about a fundamental aspect of *Morrison*'s holding: is a domestic transaction in a security (or a transaction in a security listed domestically) merely necessary for application of the Exchange Act, or is it both necessary and sufficient? In *Parkcentral Global Hub Ltd v. Porsche Auto Holdings SE*,[39] the Second Circuit concluded that some domestic transactions are beyond the territorial reach of Section 10(b). The plaintiffs in *Parkcentral* were international hedge funds that entered

'[t]he location . . . of the buyer, seller, or broker will not necessarily establish the situs of the transaction.' *In re Petrobas Sec.*, 862 F.3d 250, 262 (2d Cir. 2017). The case of *United States v. Boustani* implicated this tension. The DOJ initially contended that its indictment alleged domestic transactions because 'United States investors purchased [the relevant securities] while physically present in the United States.' Memorandum in Opposition 15–17, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 22 Jul. 2019), ECF No. 113. The defendant argued that this fact alone did not establish domesticity, and that the relevant transactions occurred abroad because they were settled and cleared in Europe. Memorandum of Law in Support of Motion to Dismiss 19–24, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 21 Jun. 2019), ECF No. 98. Before the Court decided the issue, the government obtained a superseding indictment, which alleged that 'investors in the United States incurred irrevocable liability in the United States by purchasing the [securities] while physically present in the United States'. Supplemental Memorandum in Opposition 14–15, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 13 Sep. 2019), ECF No. 166. The defendant's motion to dismiss the indictment was denied. Decision & Order, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 3 Oct. 2019), ECF No. 231. On 2 December, the jury acquitted the defendant on all counts. The defence had argued that 'the US is not the world's policeman'. Three jurors later told press that they could not see 'how federal prosecutors in Brooklyn had the authority to prosecute crimes that hadn't occurred in their jurisdiction'. Patricia Hurtado, 'Salesman Cleared in US$2 Billion African Scam in Blow to US', Bloomberg (2 Dec. 2019), available at https://www.bloomberg.com/news/articles/2019-12-02/privinvest-salesman-is-acquitted-of-defrauding-u-s-investors.

36 See SEC v. Morrone, 997 F.3d 52, 59–60 (1st Cir. 2021); *Stoyas*, 896 F.3d at 947–49; *Georgiou*, 777 F.3d at 137.

37 *Stoyas*, 896 F.3d at 949. In *Banco Safra S.A. Cayman Islands Branch v. Samarco Mineracao S.A.*, No. 19-3976-cv, 2021 WL 825743 (2d Cir. 4 Mar. 2021) (Summary Order), the Second Circuit emphasised that conclusory allegations are insufficient to satisfy the domestic transactions test, and that '[d]etailed factual allegations describing contract formation in the United States' are required. Id. at *2.

38 See *SEC v. Ahmed*, 308 F. Supp. 3d 628, 660–64 (D. Conn. 2018) (summarising cases applying the Second Circuit's standard in a variety of factual circumstances).

39 763 F.3d 198 (2d Cir. 2014).

© Law Business Research 2021

securities-based swap agreements in the United States.[40] These instruments were pegged to the price of Volkswagen shares, but the shares themselves were traded only on foreign exchanges, and the foreign defendant (which had allegedly engaged in fraud, primarily in Germany, affecting the price of shares) was not a counterparty to any of the agreements.[41] The court acknowledged that the relevant transactions had occurred in the United States, but nonetheless concluded that the case was extraterritorial. If the suit proceeded, 'it would permit the plaintiffs, by virtue of an agreement independent from the reference securities, to hale the European participants in the market for German stocks into US courts and subject them to US securities laws'.[42] This would be incompatible with *Morrison*.

In *Stoyas v. Toshiba Corp*, the Ninth Circuit disagreed. *Toshiba*, like *Parkcentral*, involved American depository receipts (ADRs), issued by United States depositary institutions without defendant Toshiba's formal participation and representing a beneficial interest in, not legal ownership of, Toshiba shares.[43] The plaintiffs alleged that Toshiba had engaged in fraud overseas, causing the value of its shares (and the value of plaintiffs' ADRs) to decrease. It appeared that plaintiffs had purchased the ADRs in the United States.[44] But Toshiba argued that the case was nonetheless extraterritorial. As in *Parkcentral*, there was 'no connection between Toshiba and the Toshiba ADR transactions', making the dispute so overwhelmingly foreign as to require dismissal.[45] The Ninth Circuit disagreed. The court wrote that *Parkcentral* was distinguishable on several grounds, but that, in any event, it was wrongly decided: the Second Circuit's approach replaced *Morrison*'s bright-line transactional test with an

40 Id. at 207.

41 Id. at 206–08.

42 Id. at 214–17. After *Parkcentral*, some Second Circuit decisions distinguished or ignored the case, casting doubt on its continued relevance. See, e.g., *Giunta v. Dingman*, 893 F.3d 73, 82 (2d Cir. 2018); *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60, 66 (2d Cir. 2018). But in 2019, in a case arising under the Commodity Exchange Act, the court both reaffirmed *Parkcentral* and extended it to that new statutory context. See *Prime Int'l Trading, Ltd. v. BP P.L.C.*, 937 F.3d 94, 104-07 (2d Cir. 2019). And in January 2021, the Second Circuit once again applied *Parkcentral*'s ''predominantly foreign' exception and concluded that § 10(b) claims based on a private offering between a Bermudan investor and a Bermudan issuer were impermissibly extraterritorial, even though the alleged misstatements were made from New York and the subscription agreement was countersigned there. See *Cavello Bay Reinsurance Ltd. v. Stein*, 986 F.3d 161, 167–68 (2d Cir. 2021).

43 *Stoyas*, 896 F.3d at 940–41.

44 Id. at 949.

45 Id..

© Law Business Research 2021

undefined standard asking whether (notwithstanding a domestic transaction) a case was 'too foreign' for US adjudication.[46]

In *SEC v. Morrone*, the First Circuit sided with the Ninth Circuit and rejected *Parkcentral*'s 'predominantly foreign' exception as inconsistent with *Morrison*.[47] In *Morrone*, the SEC filed a complaint against Bio Defense Corporation and several of its senior executives for alleged violations of the federal securities laws in connection with sales of the company's securities to foreign investors.[48] The district court held that the federal securities laws applied to the stock sales because Bio Defense incurred irrevocable liability for them in Boston, Massachusetts, where Bio Defense's founder countersigned the subscription agreements at issue, and the First Circuit affirmed.[49] In doing so, the First Circuit rejected the defendants' argument that the SEC's claims were 'predominantly foreign' under *Parkcentral* and therefore outside the reach of the federal securities laws, concluding that '[t]he existence of a domestic transaction suffices to apply the federal securities laws under *Morrison*. No further inquiry is required'.[50]

The Supreme Court declined to review the Ninth Circuit's *Stoyas* decision, and the defendants did not file a petition for a writ of *certiorari* in *Morrone*, leaving the circuit conflict unresolved. As it stands, the practical importance of the disagreement is unclear. The Ninth Circuit indicated that in the unusual circumstances present in *Parkcentral* and *Stoyas* – namely a foreign defendant drawn into a US lawsuit based solely on domestically traded derivative instruments – other elements of Section 10(b), such as the requirement that fraud be 'in connection with' the purchase or sale of a security, might preclude liability.[51]

Criminal versus civil cases 29.3

In *Morrison*, the Supreme Court described the applicability of the presumption against extraterritoriality in unequivocal terms: 'Rather than guess anew in each case, we apply the presumption in all cases.'[52] That blanket pronouncement sits uneasily with *United States v. Bowman*,[53] a 1922 decision holding that the presumption is inapplicable in certain classes of criminal cases. Neither *Morrison* nor any of the Court's other recent extraterritoriality decisions arose in the criminal context, creating uncertainty about how the Court's aggressive application of the presumption translates to criminal prosecutions.

46 Id. at 950. See *In re Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Product Liability Litigation*, _ F. Supp. 3d _ 2020 WL 4905093, at *11 (N.D. Cal. 20 Aug. 2020) ('what matters is not the foreign character of [a defendant's] conduct but whether the SEC has adequately alleged a nexus between that conduct and the bond offerings').

47 997 F.3d at 60.

48 Id. at 58.

49 Id. at 58–61.

50 Id. at 60.

51 *Stoyas*, 896 F.3d at 950–52.

52 *Morrison*, 561 U.S. at 261.

53 260 U.S. 94 (1922).

© Law Business Research 2021

The defendants in *Bowman* schemed to defraud a government-owned company, acting on the high seas and in Brazil.[54] The Court acknowledged the presumption against extraterritoriality and stated that it applied to '[c]rimes against private individuals or their property, like assaults, murder, burglary, larceny, robbery, arson, embezzlement, and frauds of all kinds'.[55] But, the Court reasoned, 'the same rule of interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated'.[56] In such cases, Congress need not speak clearly for its statute to apply extraterritorially, for it has allowed it 'to be inferred' from the 'nature' of the offence.[57]

By its terms, the *Bowman* exception was drawn narrowly.[58] But in the decades that followed, the courts of appeals 'applied *Bowman* . . . with varying degrees of liberality'[59] and many courts held *Bowman* applicable (and the presumption against extraterritoriality inoperative) in circumstances well removed from 'criminal statutes . . . enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated'.[60] For example, some courts drew on *Bowman*'s reference to the nature of the crime to exempt whole classes of criminal statutes that frequently involve transnational conduct or effects, such as 'immigration . . . , sex tourism and human trafficking, and drug trafficking'.[61]

The Court's reinvigorated commitment to the presumption against extraterritoriality suggests that, in an appropriate case, it might be willing to revisit *Bowman*. In the meantime, lower courts have not been willing to conclude that *Bowman* has been impliedly overruled.[62] The government has read *Bowman* broadly to argue that cases like *Morrison* and *RJR Nabisco* simply do not apply in criminal matters. Lower courts have not been receptive to that argument either.[63] Instead, the question in lower courts has been the extent of the *Bowman*

54 Id. at 95–97.

55 Id. at 98.

56 Id.

57 Id.

58 Id. at 98–99.

59 *United States v. McVicker*, 979 F. Supp. 2d 1154, 1171 (D. Or. 2013).

60 *Bowman*, 260 U.S. at 98.

61 Zachary D Clopton, 'Bowman Lives: The Extraterritorial Application of U.S. Criminal Law After Morrison v. National Australia Bank', 67 *N.Y.U. Ann. Surv. Am. L.* 137, 169–70 (2011); see id. at 170 nn. 135–37 (collecting cases).

62 e.g., *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 91 n. 5 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 2018).

63 See, e.g., *United States v. Vasquez*, 899 F.3d 363, 374 (5th Cir. 2018) (rejecting the 'puzzling position' that '*RJR Nabisco* does not apply to criminal cases'); *United States v. Vilar*, 729 F.3d 62, 72 (2d Cir. 2013) ('no plausible interpretation of *Bowman*' supported the government's argument that 'the presumption against extraterritoriality has no place in our reading of

© Law Business Research 2021

exception in light of the Court's recent extraterritoriality decisions. Many have applied the presumption in criminal cases while acknowledging that there is tension between *Morrison* and *Bowman* or, at a minimum, explaining that *Morrison* highlights the need to confine *Bowman*'s exception to narrow limits.[64]

However lower courts navigate the *Bowman–Morrison* tension as a general matter, *Morrison* appears to bear directly on the interpretation of 'hybrid' statutes, namely statutes that apply both criminally and civilly. As a rule, federal courts construe hybrid statutes consistently across applications, rather than interpret the same statute one way in criminal cases and another in civil cases.[65] *Morrison* makes clear that the presumption against extraterritoriality (1) applies universally in (at least) the civil context, and (2) is a rule of statutory construction.[66] Therefore, under *Morrison*, statutes capable of civil application should be construed using the presumption against extraterritoriality, generating an interpretation that applies perforce if the statute is also capable of criminal application. Indeed, as the Second Circuit held in *Vilar*, the statute construed in *Morrison* – Section 10(b) – is itself a hybrid statute and after *Morrison* lacks extraterritorial effect in both its civil and criminal dimensions.[67]

---

criminal statutes'). See also *United States v. Sota*, 948 F.3d 356, 358–59, 361–62 (D.C. Cir. 2020) (rejecting the government's argument that the statute prohibiting murder of US employees while engaged in official duties should have extraterritorial reach).

64 See, e.g., *Vasquez*, 899 F.3d at 373–74 & n.6; *Vilar*, 729 F.3d at 72–74; *All Assets*, 251 F. Supp. 3d at 91 n. 5; *United States v. Abu Khatallah*, 151 F. Supp. 3d 116, 124–26 (D.D.C. 2015) (explaining that *Bowman* 'sits uneasily with *Aramco*, *Morrison*, and *Kiobel*'). But not all courts have embraced the idea that the Court's recent extraterritoriality cases bear on the *Bowman* exception. See, e.g., *United States v. Leija-Sanchez*, 820 F.3d 899, 901 (7th Cir. 2016) ('A decision such as *Bowman*, holding that criminal and civil laws differ with respect to extraterritorial application, is not affected by yet another decision showing how things work on the civil side [i.e., *Morrison*].').

65 See, e.g., *Leocal v. Ashcroft*, 543 U.S. 1, 12 n. 8 (2004) ('[W]e must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context.'); *FCC v. Am. Broadcast Co.*, 347 U.S. 284, 296 (1954) ('There cannot be one construction for the Federal Communications Commission and another for the Department of Justice.'); *Carter v. Welles-Bowen Realty, Inc.*, 736 F.3d 722, 727 (6th Cir. 2013) ('A single statute with civil and criminal applications receives a single interpretation.'). Notwithstanding the Supreme Court's apparently clear statements on this matter, some cases contravene or call into question the rule of consistent interpretation. See, e.g., *United States v. Plaza Health Labs, Inc.*, 3 F.3d 643, 648 (2d Cir. 1993); see also *Babbitt v. Sweet Home Chapter of Communities for a Greater Oregon*, 515 U.S. 687, 704 n. 18 (1995) (deferring to an agency interpretation of a law carrying criminal penalties, and suggesting that the rule of lenity had no application because the case arose in a civil context).

66 See *Vilar*, 729 F.3d at 74.

67 Id. ('[E]ven if it were the case that we do not generally apply the presumption against extraterritoriality to criminal statutes, Section 10(b) would still not apply extraterritorially in criminal cases. The reason is simple: The presumption against extraterritoriality is a method of interpreting a statute, which has the same meaning in every case.'); see *Vasquez*, 899 F.3d at 373 n. 6 (applying *RJR Nabisco* to a criminal RICO case, and explaining that RICO 'is a

© Law Business Research 2021

29.4 RICO

The Racketeer Influenced and Corrupt Organizations Act (RICO) prohibits engaging in 'a pattern of racketeering activity' in relation to an enterprise.[68] 'The statute defines "racketeering activity" to encompass dozens of state and federal offenses, known in RICO parlance as predicates.'[69] Violations of RICO's substantive prohibitions are subject to criminal prosecution and civil enforcement proceedings.[70] In addition, RICO creates an express private right of action for '[a]ny person injured in his business or property by reason of a violation of Section 1962'.[71]

See Chapter 26 on fines, disgorgement, etc.

The Supreme Court considered RICO's extraterritorial scope in *RJR Nabisco*, a civil action brought by the European Community and 26 of its Member States against defendants alleged to have 'participated in a global money-laundering conspiracy in association with various organized crime groups'.[72] The Court reached three significant conclusions. First, it held that RICO overcomes the presumption against extraterritoriality because certain predicates apply extraterritorially, 'a clear, affirmative indication that Section 1962 applies to foreign racketeering activity'.[73] But 'when a statute provides for some extra-territorial application, the presumption against extraterritoriality operates to limit that provision to its terms'.[74] Therefore, RICO applies extraterritorially 'only to the extent that the predicates alleged in a particular case themselves apply extraterritorially'.[75] Second, the Court held that – even where an alleged predicate offence applies extraterritorially – RICO's substantive prohibitions require 'proof of an enterprise that is "engaged in, or the activities of which affect, interstate or foreign commerce"'.[76] This necessary link to US commerce provides a further limit on RICO's extraterritorial scope. Third, the Court held that RICO's private right of action has no extraterritorial application, even in cases involving extraterritorial predicates.[77] 'A private RICO plaintiff therefore must allege and prove a domestic injury to its business or property.'[78]

---

hybrid statute authorizing criminal prosecution, civil enforcement, and private civil actions' (internal citations omitted)); see id. (collecting criminal RICO cases that apply *RJR Nabisco*).

68 *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2096–97 (2016); see 18 U.S.C. § 1962.

69 *RJR Nabisco*, 136 S. Ct. at 2096.

70 18 U.S.C. §§ 1963(a), 1964(a)–(b).

71 *RJR Nabisco*, 136 S. Ct. at 2097 (quoting 18 U.S.C. § 1964(c)).

72 Id. at 2098.

73 Id. at 2102.

74 Id. (quoting *Morrison*, 561 U.S. at 265).

75 Id.

76 Id. at 2105 (quoting 18 U.S.C. § 1962(a)–(c)).

77 Id. at 2106.

78 Id.

© Law Business Research 2021

A number of courts have applied *RJR Nabisco* in the context of criminal prosecutions.[79] In a criminal case, where the domestic-injury requirement applicable to private plaintiffs has no operation, extraterritorial application will turn on the reach of the alleged predicates and the nexus between the enterprise and US commerce.[80]

Wire fraud 29.5

The wire fraud statute, 18 USC Section 1343, prohibits wire transmissions 'in interstate or foreign commerce . . . for the purpose of executing' a scheme to defraud. Federal prosecutors have broadly applied this statute to reach a variety of fraudulent conduct. Questions of the extraterritoriality of the wire fraud statute arise not only in criminal prosecutions, but also in civil cases, particularly RICO suits in which wire fraud is alleged as a predicate act.

Courts disagree about whether Section 1343 applies extraterritorially. In *United States v. Georgiou*,[81] the Third Circuit held that it does. The court relied on *dicta* from *Pasquantino v. United States*,[82] in which the Supreme Court stated that 'the wire fraud statute punishes frauds executed in "interstate or foreign commerce", so this is surely not a statute in which Congress had only "domestic concerns in mind"'.[83] But the Second Circuit rejected that view in *European Community v. RJR Nabisco, Inc.*[84] The court acknowledged the *dicta* in *Pasquantino* but reasoned that it had been abrogated by *Morrison*, which held that 'a general reference to foreign commerce . . . does not defeat the presumption against extraterritoriality'.[85] After concluding that the statute had no extraterritorial application, however, the Second Circuit left unsettled the second step of the inquiry (i.e., the focus, and therefore the domestic reach, of Section 1343) by disclaiming any need to decide 'precisely how to draw the line between domestic and extraterritorial applications of the wire fraud statute'.[86] The court reasoned that the defendants were alleged to have satisfied

79 See, e.g., *United States v. Vasquez*, 899 F.3d 363, 373 n.6 (5th Cir. 2018) (citing *United States v. Sitzmann*, 893 F.3d 811, 822 (D.C. Cir. 2018) (*per curiam*); *United States v. Ubaldo*, 859 F.3d 690, 700–01 (9th Cir. 2017); *United States v. Valenzuela*, 849 F.3d 477, 484–85 & n. 3 (1st Cir. 2017); *United States v. Gasperini*, 729 F. App'x 112, 113–14 (2d Cir. 2018)); *United States v. Harris*, 991 F.3d 552, 558–60 (4th Cir. 2021).

80 See, e.g., *United States v. Hawit*, No. 15-cr-252-PKC, 2017 WL 663542, at *9–10 (E.D.N.Y. 17 Feb. 2017).

81 777 F.3d 125 (3d Cir. 2015).

82 544 U.S. 349 (2005).

83 Id. at 371–72 (internal citation omitted). This statement was made *obiter* in that the Court held that the case involved a domestic application of the statute. Id.

84 764 F.3d 129 (2d Cir. 2014), rev'd on other grounds sub nom. *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

85 Id. at 141 (quoting *Morrison*, 561 U.S. at 263).

86 Id. at 142.

© Law Business Research 2021

each element of the statute through conduct in the United States; accordingly, 'wherever [the] line should be drawn', the case fell on the domestic side of it.[87]

After *European Community*, district courts – particularly district courts within the Second Circuit – struggled to define the kind and degree of domestic conduct necessary for application of the wire fraud statute. In *Laydon v. Mizuho Bank, Ltd*,[88] defendants acting abroad were alleged to have manipulated benchmark interest rates through fraudulent submissions to entities in London and Tokyo.[89] The court rejected the idea that mere use of the domestic wires in connection with the fraud was sufficient without proof that the scheme was managed from or directed to the United States.[90] Yet in *United States v. Hayes*,[91] another benchmark manipulation case, the court stated without qualification that using 'domestic wires to carry out [a] fraudulent scheme' is 'clearly sufficient' for domestic application. Some courts tried to explain this apparent divergence on the ground that *Laydon* was civil and *Hayes* criminal.[92] But the court in *United States v. Gasperini*,[93] a criminal case, applied a *Laydon*-like analysis to hold that the focus of the wire fraud statute is 'the scheme to defraud', and that domestic application of Section 1343 requires 'a substantial amount of conduct in the United States' that is 'integral to the commission of the scheme'.[94]

After several years of confusion, the Second Circuit imposed a measure of order in *Bascuñán v. Elsaca*.[95] *Bascuñán* was a civil RICO case (with a wire fraud predicate) in which the plaintiff alleged that the defendant, acting abroad, had fraudulently used domestic wires to obtain funds from New York bank accounts.[96] The Second Circuit noted that the critical issue, the focus of the wire fraud statute 'for the purpose of the presumption against extraterritoriality [was] a question of first impression in [the] circuit'.[97] The court rejected the view that the wire fraud statute gives way unless the scheme to defraud is 'planned, managed, and directed' from the United States.[98] It reasoned that the focus of Section 1343 'is not merely a scheme to defraud, but more precisely the use of the . . . wires in furtherance of a scheme to defraud'.[99] The court went

87 Id.

88 No. 12-cv-3419-GBD, 2015 WL 1515487 (S.D.N.Y. 31 Mar. 2015).

89 Id. at *1, *9.

90 Id. at *8–9.

91 99 F. Supp. 3d 409 (S.D.N.Y. 2015).

92 See *Sonterra Cap. Master Fund v. Credit Suisse Grp.*, 277 F. Supp. 3d 521, 581 (S.D.N.Y. 2017); see also *FrontPoint Asian Event Driven Fund, L.P. v. Citibank, N.A.*, No. 16-cv-5263-AKH, 2017 WL 3600425, at *15 (S.D.N.Y. 18 Aug. 2017).

93 No. 16-cr-441-NGG, 2017 WL 2399693 (E.D.N.Y. 1 Jun. 2017).

94 Id. at *7–8; see also *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 103 (D.D.C. 27 Apr. 2017) (applying the same test).

95 927 F.3d 108 (2d Cir. 2019).

96 Id. at 112–15, 123.

97 Id. at 121.

98 Id. at 121, 123.

99 Id. (internal quotation marks and original emphasis omitted).

© Law Business Research 2021

on to observe that the Supreme Court, and other courts of appeals, 'though not in the context of applying the presumption against extraterritoriality [had] described the focus' of the wire fraud statute in precisely those terms.[100] But not just any wire furthering a scheme would do. Because 'incidental' domestic conduct is not enough to trigger United States law, use of the wires 'must be essential' to, or 'a core component of', the scheme to defraud.[101] Applying this standard to the facts was straightforward, in that the defendant allegedly had used domestic wires to fraudulently 'transfer millions of dollars' out of domestic bank accounts – clearly a core component of the scheme.[102]

Bascuñán therefore goes some distance towards resolving the confusion that persisted after *European Community*. The Second Circuit recently made clear that *Bascuñán* extends to the honest services fraud conspiracy.[103] In addition, it remains to be seen whether other courts of appeals will follow *Bascuñán* and its 'core component' test. The First, Sixth and Ninth Circuits have all followed *Bascuñán* and concluded that the focus of the wire fraud statute is the use of domestic wires in furtherance of a scheme to defraud rather than the scheme itself.[104] The First Circuit, in *dicta*, seemingly endorsed the core component test for use in cases where 'a foreign defendant is alleged to have committed wire fraud against a foreign victim'.[105] The Ninth Circuit noted the core component test in *United States v. Hussain* and found the test satisfied by the facts of that case, without explicitly adopting the test.[106]

Commodity Exchange Act 29.6

The Commodity Exchange Act (CEA), enforced by the Commodity Futures Trading Commission (CFTC), regulates markets in commodities. This broad category embraces 'all services, rights and interests . . . in which contracts for future delivery are presently or in the future dealt in', covering not only

100 Id. at 122 (citing *Skilling v. United States*, 561 U.S. 358, 369 n. 1 (2010); *United States v. Garlick*, 240 F.3d 789, 792 (9th Cir. 2001); *United States v. Alston*, 609 F.2d 531, 536 (D.C. Cir. 1979); *United States v. Jefferson*, 674 F.3d 332, 336 (4th Cir. 2012)).

101 Id. at 122–23.

102 Id. at 123.

103 See *United States v. Napout et al.*, 963 F.3d 163 (2d Cir. 2020).

104 See *United States v. McLellan*, 959 F.3d 442, 470–71 (1st Cir. 2020) ('its focus is not the fraud itself but the abuse of the instrumentality in furtherance of a fraud'); *United States v. Hussain*, 972 F.3d 1138,1145 (9th Cir. 2020) ('the focus of the wire fraud statute, 18 U.S.C. 1343, is the use of the wires in furtherance of a scheme to defraud'); *United States v. Coffman*, 574 F. App'x 541, 558 (6th Cir. 2014) (unpublished) ('[W]ire fraud occurs in the United States when defendants use interstate wires as part of their scheme.').

105 *McLellan*, 959 F.3d at 970, n. 7.

106 *Hussain* 972 F.3d at 1143, n. 2; see *Bascuñán*, 927 F.3d 108 (2d Cir. 2019) at 121–23.

© Law Business Research 2021

traditional commodities like agricultural products,[107] but 'currency and other financial instruments'.[108]

The CEA is aimed at protecting the 'individual investor – who may know little about the intricacies and complexities of the commodities market – from being deceived or misled'.[109] To that end, the statute contains several antifraud provisions.[110] Section 22(a) of the CEA 'establishes a private right of action for individual litigants in four, limited circumstances';[111] in addition, the CFTC may pursue violations through enforcement actions, and the DOJ may bring criminal charges for certain violations.

'Prior to *Morrison*, courts deciding commodities cases applied the same conduct or effects test as was used in the securities context.'[112] But *Morrison* prompted courts to revisit those precedents. In *Loginovskaya v. Batratchenko*,[113] the Second Circuit held that the CEA's private right of action provision, Section 22, 'is silent as to extraterritorial reach' and therefore lacks extraterritorial application.[114] The court then considered the provision's domestic reach. It concluded that the focus of Section 22 is on transactions in commodities, just as the focus of Section 10(b) was found in *Morrison* to be transactions in securities. Accordingly, the court concluded, private suits under the CEA 'must be based on transactions occurring in the territory of the United States'.[115] The court further held that in determining whether a given transaction is domestic, the irrevocable liability test developed in the securities context should govern.[116] Therefore, in the Second Circuit, a transaction in a commodity will be regarded as domestic if 'the transfer of title or the point of irrevocable liability . . . occurred in the United States'.[117] Courts applying this standard have stressed the need for plaintiffs to plead and prove facts demonstrating 'the location of the transactions' at issue, including 'the formation of . . . contracts,

107 7 U.S.C. § 1a(9).

108 *Salomon Forex Inc. v. Tauber*, 795 F. Supp. 768, 771 (E.D. Va. 1992).

109 *Loginovskaya v. Batratchenko*, 936 F. Supp. 2d 357, 363 (S.D.N.Y. 2013), aff'd, 764 F.3d 266 (2d Cir. 2014).

110 Id.

111 Id. at 364.

112 Id. at 367.

113 764 F.3d 266 (2d Cir. 2014).

114 Id. at 271.

115 Id. at 272. The Second Circuit observed in a later case that the relevant portion of the CEA 'does not contain language similar to the language in § 10(b) that led *Morrison* to craft the "domestic exchange" prong' of its two-pronged test for domestic application (i.e., transactions in securities registered on domestic exchanges, or domestic transactions in other securities).' *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60, 67 (2d Cir. 2018). The court 'le[ft] aside whether *Morrison*'s discussion of exchanges is applicable to the CEA', concluding that the 'domestic transaction' test was satisfied on the facts before it. Id.

116 See *Loginovskaya*, 764 F.3d at 274; supra Section 29.2.2.

117 Id.

© Law Business Research 2021

the placement of orders, the passing of title and the exchange of money'.[118] It is insufficient for the plaintiff to show that he or she is a 'US resident who engaged in . . . futures transactions' from the United States, without proof of 'the location of the transactions themselves'.[119] In addition, the Second Circuit has extended the rule of *Parkcentral*,[120] originally developed in the securities context, to CEA cases. A domestic transaction is therefore necessary but not sufficient for an action under Section 22.[121]

Loginovskaya's statement that Section 22 is 'silent as to extraterritorial reach' is subject to a potential qualification.[122] As the court observed, Dodd-Frank amendments to the CEA altered the statute's reach in a limited set of cases:

> *[Dodd-Frank] amended CEA Section 22 to cover swaps, and provided that its 'provisions . . . relating to swaps' may, under certain circumstances, 'apply to activities outside the United States'*.[123]

Specifically, the CEA provisions regulating swaps apply to activities outside the United States that (1) 'have a direct and significant connection with activities in, or effect on, commerce of the United States', or (2) contravene CFTC rules or regulations aimed at preventing 'the evasion of any provision' added to the CEA through Dodd-Frank.[124] Because *Loginovskaya* did not involve swaps, the court took 'no view of the effect that the Dodd-Frank amendments may have on the extraterritorial reach of the CEA'.[125]

---

118 *Sullivan v. Barclays PLC*, No. 13-cv-2811-PKC, 2017 WL 685570, at *29 (S.D.N.Y. 21 Feb. 2017).

119 Id.

120 See *Park Central*, 763 F.3d 198 (2d Cir. 2014); supra Section 29.2.2.

121 See *Prime Int'l*, 937 F.3d 104–07. *Prime Int'l* was similar to *Parkcentral* in that the plaintiffs, acting in the United States, traded derivatives pegged to a foreign asset, whose price was allegedly affected by purely foreign conduct (producing losses on the domestic derivatives trades). Id. at *2–3, *8. The court held that plaintiffs were required to show not only a domestic transaction that would satisfy § 22, but domestic conduct that violated a substantive, conduct-regulating provision of the CEA. Id. at *7.

122 764 F.3d at 271.

123 Id. at 271 n. 4.

124 7 U.S.C. § 2(i). Dodd-Frank's limited revision of the extraterritorial reach of the CEA stands in contrast to its (attempted) wholesale revision of the extraterritorial reach of the Exchange Act: While § 929P of Dodd-Frank appears aimed at restoring the conduct-and-effects test in all SEC and criminal actions under the anti-fraud provisions of the Exchange Act, see supra Section 29.2.2, no such sweeping provision was made for CEA cases.

125 764 F.3d at 271 n. 4. The Second Circuit again declined to consider the effect of Dodd-Frank's swaps provisions in *Prime Int'l* 937 F.3d at 103–04, concluding that the plaintiffs had forfeited the argument that the CEA applied extraterritorially on that basis. See id.

© Law Business Research 2021

Some questions of extraterritoriality play out differently in the context of enforcement actions, as opposed to private actions.[126] To begin, several provisions in the CEA expressly grant the CFTC regulatory and enforcement authority over certain conduct involving foreign elements. The statute permits the CFTC to adopt rules proscribing fraud concerning transactions or instruments made on or subject to the rules of foreign exchanges or markets, so long as the regulated behaviour is committed by 'any person located in the United States'; it also grants the Commission authority to enforce those rules through lawsuits.[127]

In addition, because enforcement actions do not rely on the transaction-focused private right of action in Section 22, it is likely that some such actions will be permitted to proceed as domestic applications of the CEA based on territorial connections other than US transactions. For example, the Second Circuit has held that the anti-fraud provisions Sections 6(c)(1)[128] and 9(a)(2)[129] centre on manipulation of commodities markets and prices, not on transactions.[130] Similarly, Section 4o, another anti-fraud provision, prohibits commodity trading advisers, and associated individuals or entities, from defrauding clients – without any requirement that the fraud occur in connection with a transaction in a commodity.[131] Given that the provision is not transaction-based, there appears to be no warrant for applying *Morrison*'s 'domestic transaction' test in this context.[132]

29.7 Antitrust

On its face, the Sherman Act proscribes 'every contract, combination . . . or conspiracy in restraint of trade', but the Supreme Court has held that the Act 'outlaw[s] only *unreasonable* restraints'.[133] Most trade practices are evaluated under the rule of reason, which requires a determination whether, in all the circumstances, 'a restrictive practice should be prohibited as imposing

126 See id. ('[T]he CEA draws a distinction between the extraterritoriality limits on a private action and enforcement actions brought by the CFTC itself.'); *CFTC v. Vision Fin. Partners, LLC*, 19 F. Supp. 3d 1126, 1131 (S.D. Fla. 2016) (distinguishing, for purposes of extraterritoriality, between private actions and 'suits brought by the Commission itself').

127 *Vision Fin. Partners, LLC*, 190 F. Supp. 3d at *1131 (quoting 7 U.S.C. § 6(b)(2)).

128 'It shall be unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance'. 7 U.S.C. § 9(a)(1).

129 'It shall be a felony . . . for . . . [a]ny person to manipulate or attempt to manipulate the price of any commodity in interstate commerce' 7 U.S.C. § 13(a)(2).

130 *Prime Int'l*, 937 F.3d at 107–08.

131 *Loginovskaya*, 936 F. Supp. 2d at 368.

132 Id. at 369 ('*Morrison*'s transaction test is not immediately applicable to § 4o.').

133 *Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 885 (2007) quoting 15 U.S.C. § 1 (emphasis added).

© Law Business Research 2021

an unreasonable restraint on competition'.[134] But horizontal cartel activity – outright collusion among competitors – is a *per se* violation of the Sherman Act.[135] The antitrust laws are enforced both civilly and criminally, with criminal enforcement generally limited to *per se* violations.[136]

In *Hartford Fire Insurance Co v. California*, decided in 1993, the Supreme Court declared it 'well established by now that the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States'.[137] That formulation tracked the 'effects' test that *Morrison* would reject in 2010.[138] Arguably, then, *Morrison* may be read to have called into question the continued vitality of *Hartford Fire*.[139]

But *Morrison* has not prompted broad reconsideration of the extraterritorial reach of the Sherman Act, likely for two reasons. First, it may be possible to harmonise *Morrison* and *Hartford Fire*. In *Morrison*, it was held that lower courts had been wrong not to apply the presumption against extraterritoriality in cases where the effects test was satisfied, and should in the future apply the presumption in all cases.[140] One reading of *Hartford Fire* is that the presumption against extraterritoriality is rebutted in Sherman Act cases; that is, the Court's 'effects' language was offered not as a reason to avoid applying the presumption (which would contravene *Morrison*), but as a description of the extraterritorial reach of a statute that overcomes the presumption. Although the majority did not say as much (or mention the presumption at all), the author of the decision, Justice Scalia, took that view in dissent: 'We have . . . found the presumption to be overcome with respect to our antitrust laws.'[141]

Second, when Congress adopted the Foreign Trade Antitrust Improvements Act (FTAIA), it 'expressly endorsed an extraterritorial application of the Sherman Act'.[142] The FTAIA first provides that all foreign commercial activity (except import commerce, namely commerce between foreign sellers and

134 Id. (internal quotation marks omitted).

135 Id. at 893.

136 See D. Daniel Sokol, *Reinvigorating Criminal Antitrust?*, 60 Wm. & Mary L. Rev. 1545, 1572–73 (2019).

137 509 U.S. 764, 795–96 (1993).

138 See *Schoenbaum v. Firstbrook*, 405 F.2d 200, 208 (2d Cir. 1968) (citing *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443–44 (2d Cir. 1945)).

139 See Julie Rose O'Sullivan, 'The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusion, and a Plea to Congress for Direction', 106 *Geo. L.J.* 1021, 1049–52 (2018) (noting apparent tension between the Court's antitrust cases and *Morrison*).

140 See *Morrison*, 561 U.S. at 256–61.

141 *Hartford Fire*, 509 U.S. at 813.

142 *Sonterra Cap. Master Fund v. Credit Suisse Grp.*, 277 F. Supp. 3d 521, 569 (S.D.N.Y. 2017) (internal quotation marks omitted). The FTAIA provides an independent basis for extraterritorial application of the antitrust laws – separate from *Hartford Fire* – because *Hartford Fire* expressly disclaimed any reliance on the FTAIA. 509 U.S. at 796 n. 23.

© Law Business Research 2021

domestic buyers) is 'outside the Sherman Act's reach', but then 'brings such conduct back within' the Act if:[143]

> *(1) the foreign conduct has a 'direct, substantial, and reasonably foreseeable effect' on US domestic, import or certain export commerce; and (2) that effect 'gives rise to a claim under' the Sherman Act.*[144]

This standard is similar (but not identical) to *Hartford Fire*'s rule.[145] Therefore, in antitrust cases involving foreign conduct, there are two related but conceptually distinct paths to extraterritorial application. Foreign activity not subject to the FTAIA (i.e., import commerce) is tested under *Hartford Fire*.[146] Other foreign activity is tested under the similar formulation set out in the FTAIA.[147]

It is clear, therefore, that the Sherman Act may reach extraterritorial conduct based on domestic effects. For example, in civil cases arising from the manipulation of benchmark interest rates by non-US traders working for defendant banks, courts applied the FTAIA to conclude that conduct occurring abroad was reachable where it affected the price of financial products sold domestically: '[M]anipulation of a benchmark that is globally disseminated and serves as a pricing component of derivatives sold widely in the United States . . . would have a foreseeable effect within the United States.'[148]

The case law is less clear about what domestic effects count. The Ninth Circuit has interpreted 'direct' in the first prong of the FTAIA – 'direct, substantial, and reasonably foreseeable effect' – to require that the domestic

---

143 *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 162 (2004).

144 *Lotes Co., Ltd. v. Hon Hai Precision Indus. Co.*, 753 F.3d 395, 413–14 (2d Cir. 2014) (citations omitted) (quoting 15 U.S.C. § 6a).

145 In addition to requiring that the effect on commerce be 'direct', see *United States v. LSL Biotechnologies*, 379 F.3d 672, 679–80 (9th Cir. 2004), the FTAIA eliminated the requirement that the foreign actor intend to affect US commerce – a product of Congress's determination that a subjective intent-based standard was undesirable and should be replaced with a 'single, objective test'. H.R. Rep. No. 97-686, at 2–3, 9 (1982); see *United States v. Hui Hsiung*, 778 F.3d 738, 748 (9th Cir. 2015) ('[T]he FTAIA's requirement that the defendants' conduct had a "direct, substantial, and reasonably foreseeable" effect on domestic commerce displaced the intentionality requirement of *Hartford Fire* where the FTAIA applies.').

146 See *Minn-Chem, Inc. v. Agrium, Inc.*, 683 F.3d 845, 855 (7th Cir. 2012) ('[T]he Sherman Act covers imports when actual and intended effects on US commerce have been shown. In *Hartford Fire*, the Supreme Court confirmed this rule, stating that "the Sherman Act covers foreign conduct producing a substantial intended effect in the United States".' (quoting *Hartford Fire*, 509 U.S. at 797)). Of course, for entities that direct goods into domestic commerce through importing activity, the requisite effects will generally be easily proved.

147 Id. at 855–56.

148 *Sonterra*, 277 F. Supp. 3d at 569; *Sullivan v. Barclays PLC*, No. 13-cv-2811-PKC, 2017 WL 685570, at *22 (S.D.N.Y. 21 Feb. 2017) ('Defendants also point to the Europe-based conduct of defendants, even though the FTAIA's express language and the decisions applying it focus on the anti-competitive effects within the United States.') (emphasis in original).

© Law Business Research 2021

effect follow 'as an immediate consequence of the defendant's activity'.[149] Other courts, including the Second and Seventh Circuits, have embraced what appears to be a weaker conception of directness, expressly rejecting the Ninth Circuit's position and holding that 'the term "direct" means only a reasonably proximate causal nexus'.[150] Despite this overt disagreement, however, there may be little daylight between the competing approaches. The Ninth Circuit has upheld convictions arising from a foreign price-fixing conspiracy where the conspirators fixed the prices of components that were sold abroad and then incorporated into products sold domestically, reasoning that 'the practical upshot of the conspiracy would be and was increased prices to customers in the United States'.[151] In so doing, the court approvingly quoted Seventh Circuit case law contrasting sufficiently direct effects with 'action in a foreign country [that] filters through many layers and finally causes a few ripples in the United States'.[152] In practice – although the precise contours of the rule are unclear – it appears that any of these courts would apply the FTAIA to some foreign anticompetitive conduct that is a step removed from any domestic effects.[153]

Finally, some territorial constraints on private antitrust actions may not apply, or apply differently, in enforcement or criminal actions. For example, in *Motorola Mobility LLC v. AU Optronics Corp*,[154] the Seventh Circuit held that the plaintiff's private action failed under the FTAIA requirement that domestic effects on commerce 'give rise to' the claim, as well as the indirect-purchaser doctrine.[155] But the court cautioned: 'If price fixing by the component manufacturers had the requisite statutory effect on cell phone prices in the United States, the Act would not block the Department of Justice from seeking criminal or injunctive remedies.'[156]

149 *LSL Biotechnologies*, 379 F.3d at 680.

150 *Lotes Co.*, 753 F.3d at 410 (internal quotation marks omitted); see *Minn-Chem*, 683 F.3d at 856–57 (rejecting the Ninth Circuit's test in favour of the 'reasonably proximate causal nexus' formulation).

151 *Hsiung*, 778 F.3d at 759.

152 Id. (quoting *Minn-Chem*, 683 F.3d at 860).

153 Underscoring the lack of practical difference between the two standards, the defendants in *Hsiung* filed a petition for certiorari arguing that the Ninth Circuit's conception of directness was weaker than the Seventh Circuit's. See Pet. for Certiorari 15–16, *Hsiung v. United States*, No. 14-1121 (16 Mar. 2015), cert. denied, 135 S. Ct. 2837 (15 Jun. 2015).

154 775 F.3d 816 (7th Cir. 2015).

155 Id. at 819–23.

156 Id. at 825. Indeed, the same cartel activity was successfully prosecuted in *Hsiung*. See also *Empagran*, 542 U.S. at 170–71 (concluding that plaintiffs' private action failed under the 'give rise to' requirement because their injury flowed purely from foreign effects, and distinguishing earlier cases permitting the government to seek 'relief that might have helped to protect those injured abroad' on the ground that the government enjoys 'broad' authority to 'seek to obtain the relief necessary to protect the public from further anticompetitive harm').

© Law Business Research 2021

29.8 Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act regulates certain persons and entities by proscribing bribery of foreign officials. The FCPA also prohibits issuers of US securities from falsifying its books and records.[157] As its name suggests, the FCPA applies extraterritorially.[158] But even 'when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms'.[159] The FCPA sets out with 'surgical precision' the circumstances in which its anti-bribery provisions apply.[160] Specifically, these provisions reach (1) issuers of securities registered on US exchanges or that file periodic reports with the SEC that use interstate commerce in furtherance of a bribery scheme (issuers), (2) United States companies or persons that use interstate commerce in furtherance of a bribery scheme (domestic concerns) and (3) 'foreign persons or businesses taking acts to further certain corrupt schemes, including ones causing the payment of bribes, while present in the United States'.[161] In addition, the statute reaches 'any officer, director, employee, or agent' acting on behalf of a covered entity.[162]

In published guidance and enforcement actions, the government has taken a broad view of the kind of conduct that will render a largely foreign scheme subject to US jurisdiction. Jointly published guidance from the SEC and DOJ states that the use-of-commerce requirement would be satisfied by any telephone call, email, text message or fax to the United States, or by 'sending a wire transfer . . . to a US bank or otherwise using the US banking system'.[163] The government has asserted this view in enforcement actions. For example, in *United States v. JGC Corp*, a Japanese defendant was charged with FCPA violations arising from a scheme to bribe Nigerian officials. The jurisdictional theory was that 'certain alleged bribe payments . . . flowed through US bank accounts and that co-conspirators faxed or e-mailed information into the United States

157 15 U.S.C. §§ 78dd-1–3, 78m.

158 See *United States v. Hoskins*, 902 F.3d 69, 96 (2d Cir. 2018).

159 *Morrison*, 561 U.S. at 265.

160 *Hoskins*, 902 F.3d at 84.

161 Id. at 71; see 15 U.S.C. § 78dd-1–3. The government has taken the position that the territorial jurisdiction prong of 15 U.S.C. § 78dd-3 applies to 'foreign persons . . . that, either directly *or through an agent*, engage in any act in furtherance of a corrupt payment . . . while in the territory of the United States'. Criminal Division of the US Department of Justice and Enforcement Division of the US Securities and Exchange Commission (SEC), A Resource Guide to the US Foreign Corrupt Practices Act, Second Edition (2020) (FCPA Resource Guide), at 10.

162 *Hoskins* at 71. An agent of a foreign person or business is covered only for acts that occur 'while in the territory of the United States'. 15 U.S.C. § 78dd-3.

163 FCPA Resource Guide, at 10.

© Law Business Research 2021

in furtherance of the bribery scheme'.[164] The case was resolved through a deferred prosecution agreement (DPA) so the issue was not litigated.[165]

FCPA actions are frequently resolved without adversarial litigation, through plea agreements, DPAs, non-prosecution agreements (NPAs), or SEC 'neither admit nor deny' settlements, so aggressive theories of jurisdiction have rarely been subjected to judicial scrutiny.[166] When they have been, results have been mixed. In *United States v. Patel*, the defendant was not an issuer or a domestic concern (or acting on behalf of such an entity), meaning that he was subject to the FCPA only for acts taken 'while in the territory of the United States'.[167] The government charged an FCPA count based on the defendant's mailing a DHL package from London to the United States.[168] The government acknowledged the requirement of territorial conduct, but argued that this element was satisfied based on separate conduct that formed the basis for a different count; that is, the government theorised that once any domestic conduct was proved, further FCPA counts could be charged based on purely foreign acts.[169] The court disagreed, reasoning that each charged violation had to have occurred while in US territory.[170] In *SEC v. Straub*,[171] the defendants were officers of an issuer – making the requirement of territorial conduct inapplicable – but the government still had to prove that they had used interstate commerce to further their bribery scheme.[172] The government alleged that the defendants had sent emails that were 'routed through and/or stored' on US servers.[173] The defendants argued that this element contained a *mens rea* requirement, so that conviction was improper without proof that they knew the emails would be routed through or stored in the United States.[174] The court, addressing 'a matter of first impression in the FCPA context', sided with the government, concluding that the defendants were subject to the FCPA even if they lacked knowledge that their conduct involved interstate commerce.[175]

In addition to pressing aggressive interpretations of the FCPA's textual coverage, the government has also sought to expand the statute's reach through conspiracy and complicity theories. Two recent decisions diverge on whether

164 Mike Koehler, The Foreign Corrupt Practices Act in a New Era 110 (2014); see Information 10–17, *United States v. JGC Corp.*, No. 11-cr-260 (S.D. Tex. 6 April 2011).

165 See Deferred Prosecution Agreement, *United States v. JGC Corp.*, No. 11-cr-260 (S.D. Tex. 6 Apr. 2011).

166 See Koehler, supra note 164, at 60–63.

167 15 U.S.C. § 78dd-3(a).

168 Tr. 7–10, *United States v. Patel*, No. 09-cr-335 (D.D.C. 12 August 2011), ECF No. 434.

169 Id.

170 Id. at 11, 29.

171 921 F. Supp. 2d 244 (S.D.N.Y. 2013).

172 Id. at 260, 262.

173 Id. at 262.

174 Id.

175 Id. at 263–64.

© Law Business Research 2021

the government may so employ principles of secondary liability to reach individuals who would not otherwise be subject to the FCPA. In *United States v. Hoskins*,[176] prosecutors argued that the defendant, a foreign national employed by a French company who never entered the United States during the alleged scheme, was criminally liable for conspiring with and aiding and abetting employees of his company's US subsidiary in a scheme to bribe Indonesian officials.[177] The Second Circuit rejected that view. The court reasoned that the statute's text and legislative history evinced an affirmative legislative policy to limit liability to the categories of individuals and entities described therein; the government could not override that choice by charging individuals outside those categories under conspiracy or complicity theories.[178] In any event, wrote the court, the presumption against extraterritoriality limits the FCPA's extraterritoriality provisions to their terms, and '[t]he government may not expand the extraterritorial reach of the FCPA by recourse to the conspiracy and complicity statutes'.[179] But a judge in the Northern District of Illinois expressly broke with *Hoskins* in *United States v. Firtash*,[180] concluding that Seventh Circuit precedent on conspiracy and accomplice liability commanded the opposite result.[181] The court permitted the government to proceed against two defendants, neither of whom belonged to 'the class of individuals capable of committing a substantive FCPA violation', on theories of secondary liability.[182]

At trial in *Hoskins*, the government proceeded on a theory that the defendant was an agent of a domestic concern and therefore among the class of persons subject to the FCPA. This was an aggressive theory because the defendant was employed by the French parent company, not its US subsidiary. The district court instructed the jury that an agency relationship requires the following: 'one, a manifestation by the principal that the agent will act for it; two, acceptance by the agent of the undertaking; and, three, an understanding between the agent and the principal that the principal will be in control of the undertaking'.[183] The jury convicted but the trial court set aside the FCPA counts of conviction on the basis that the government failed to prove the control prong of the agency test. The government has appealed this ruling.[184]

The statute does not by its terms extend to foreign subsidiaries of US issuers or domestic concerns. But the government's published guidance states its position that US parents may be held liable for the conduct of their

176 902 F.3d 69 (2d Cir. 2018).

177 Id. at 72–76.

178 Id. at 76–95.

179 Id. at 95–97.

180 392 F. Supp. 3d 872 (N.D. Ill. 2019).

181 Id. at *11–13.

182 Id.

183 Trial Tr. 1246–47, *United States v. Hoskins* (D. Conn. 6 Nov. 2019).

184 Jury Verdict, *United States v. Hoskins* (D. Conn. 8 Nov. 2019), ECF No. 583; *United States v. Hoskins* _ F. Supp 3d _ 2020 WL 914302 *7 (D. Conn. 26 Feb. 2020).

© Law Business Research 2021

foreign subsidiaries 'under traditional agency principles'.[185] If the government determines that there exists an agency relationship between the parent and its subsidiary – based on such factors as 'the parent's control – including the parent's knowledge and direction of the subsidiary's actions, both generally and in the context of the specific transaction', it will view the parent as 'liable for bribery committed by the subsidiary's employees'.[186]

Sanctions 29.9

Starting in earnest in the aftermath of World War I, the United States has pursued its foreign policy goals through imposition of economic sanctions, namely 'the deliberate withdrawal of normal economic relations between [the US] and a target country, government, entity, or individual in order to coerce the target to modify its behavior in a manner consistent with'US policy goals.[187] The statutory basis for most modern sanctions programmes is the International Emergency Economic Powers Act of 1977,[188] which grants the executive broad economic regulatory authority to respond to threats against 'the national security, foreign policy, or economy of the United States'.[189] US sanctions are administered by the Treasury Department's Office of Foreign Assets Control (OFAC), which may impose civil penalties for non-compliance.[190] In addition, the DOJ may seek criminal penalties for wilful violations, including imprisonment and fines up to US$1 million.[191]

See Chapter 45 on sanctions

See Chapter 26 on fines, disgorgement, etc.

Sanctions programmes 'vary greatly in scope and objective'.[192] OFAC's 'country-based' programmes are aimed at governments, and its 'list-based programmes' are targeted at specific persons.[193] Under list-based programmes, designated entities and individuals are added to OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), which is regularly updated and publicly accessible.[194] Once added to the list, '[t]heir assets are blocked and

185 FCPA Resource Guide, supra note 161, at 28.

186 Id.

187 Court E Golumbic and Robert S Ruff III, 'Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions', 38 *N.C. J. Int'l L. & Com. Reg.* 729, 731 (2013).

188 Pub. L. No. 95-223, 91 Stat. 1625 (1997), codified as amended at 50 U.S.C. §§ 1701–1707.

189 50 U.S.C. §§ 1701–1702.

190 Id. § 1705(b).

191 Id. § 1705(a), (c).

192 Golumbic and Ruff III, supra note 187, at 732; see id. at 770 (describing the operation of various programmes, from the Cuba programme's 'near total embargo on all goods and services' to programmes that 'are not tied to a geographic region, but instead target persons deemed to be engaged in' certain illicit activities).

193 Perry S. Bechky, Sanctions and the Blurred Boundaries of Int'l Economic Law, 83 *Mo. L. Rev.* 1, 4 (2018).

194 See OFAC, Specially Designated Nationals and Blocked Persons List (10 Nov. 2021), available at treasury.gov/ofac/downloads/sdnlist.pdf (last visited 10 November 2021). OFAC also maintains several non-SDN sanctions lists – collected in the Consolidated Sanctions List –

© Law Business Research 2021

US persons are generally prohibited from dealing with them'[195] unless authorised by OFAC through a licence.[196]

The territorial reach of a given sanctions programme turns on the particular regulations that define its scope. Many prohibitions apply by their terms only to 'US persons',[197] a term that includes 'any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States'.[198] Such prohibitions therefore apply on the basis of both nationality (including the foreign branches of domestic entities) and territoriality (as to foreign nationals). They are broad enough to reach any transactions made using the US financial system – even transactions beginning and terminating abroad that simply pass through domestic correspondent banks (as US dollar-denominated transactions generally do).[199] Moreover, sanctions applicable to Iran and Cuba apply even more broadly, reaching all persons 'subject to the jurisdiction of the United States' – a category embracing (in addition to US citizens or residents, persons in the United States, and US entities) any organisation owned or controlled by a US citizen, resident or entity.[200]

Secondary sanctions, a feature of several US sanctions programmes, are a cousin to extraterritorial primary sanctions.[201] Like primary sanctions (i.e., compliance obligations, the violation of which is civilly or criminally

---

including the Foreign Sanctions Evaders List and the Sectoral Sanctions Identifications List. See OFAC, List of Foreign Sanctions Evaders Sanctioned Pursuant to Executive Order 13608 (11 May 2021), available at https://www.treasury.gov/ofac/downloads/fse/fselist.pdf (last visited 10 November 2021) (including entities and individuals determined to have 'engag[ed] in conduct relating to the evasion of US economic and financial sanctions with respect to Iran or Syria'); OFAC, Sectoral Sanctions Identifications List (12 Mar. 2020), available at https://www.treasury.gov/ofac/downloads/ssi/ssilist.pdf (last visited 10 November 2021) (including 'persons determined by OFAC to be operating in' certain sectors of the Russian economy identified by the Secretary of the Treasury).

195 OFAC, Specially Designated Nationals and Blocked Persons List (SDN), available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx (last visited 10 November 2021).

196 See Golumbic and Ruff III, supra note 187, at 778 ('OFAC issues two types of licenses: (1) general licenses, which are made public and provide universal exemptions to a given set of sanctions, and (2) specific licenses, which are granted only upon application and authorize only the applicant to engage in a specific transaction or category of transaction.' (footnotes omitted)).

197 See, e.g., 31 C.F.R. § 542.206 (prohibiting new investment in Syria by a United States person).

198 See, e.g., 31 C.F.R. § 542.319 (defining the term for purposes of Syrian sanctions).

199 See *United States v. $1,071,251.44 of Funds Associated with Mingzheng Int'l Trading Ltd.*, 324 F. Supp. 3d 38, 43, 52 (D.D.C. 2018); *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 95 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 2018).

200 See 31 C.F.R. § 515.329 (Cuba); id. § 535.329 (Iran).

201 Bechky, supra note 193, at 9.

© Law Business Research 2021

punishable) that apply extraterritorially, secondary sanctions apply to conduct occurring outside the United States.[202] But unlike primary sanctions, secondary sanctions are not enforced by fines or imprisonment. Instead, secondary sanctions threaten economic restrictions on a third-party country or its citizens for certain conduct, generally transacting with a target of primary sanctions.[203] For example, the Iran Sanctions Act, enacted in 1996 and amended several times since, 'mandated the imposition of specified sanctions against foreign firms that reached threshold levels of involvement with Iran's energy sector'.[204] Such secondary sanctions are not extraterritorial in the sense of extending US regulatory jurisdiction to foreign conduct – they are not backed by coercive measures like fines or imprisonment – but they can carry significant consequences for violators, and have at times been 'condemned as "extraterritorially" illegal' by US trading partners.[205]

Money laundering 29.10

The Money Laundering Control Act (MLCA) prohibits (among other conduct) engaging in a financial transaction involving the proceeds of 'specified unlawful activity', or transporting money into or from the United States, with intent to promote or conceal specified unlawful activity.[206] The term 'specified unlawful activity' embraces more than 250 predicate offences.[207] The government need only prove that the defendant intended to promote or conceal the specified unlawful conduct, not that he or she actually committed the predicate offence (or even had the capacity to do so).[208]

Section 1956 provides that:

> *There is extraterritorial jurisdiction over the conduct prohibited by this section if: (1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and (2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.*[209]

202 See id.

203 See Jeffrey A Meyer, 'Second Thoughts on Secondary Sanctions', 30 *U. Pa. J. Int'l L.* 905, 926 (2009).

204 See *United States v. Amirnazmi*, 645 F.3d 564, 579 (3d Cir. 2011) (citing Iran Sanctions Act, Pub. L. No. 104-72, 110 Stat. 1541 (1996) (codified in part at 50 U.S.C. § 1701 (note)).

205 Meyer, supra note 203, at 929.

206 18 U.S.C. § 1956(a)(1), (2).

207 *United States v. Santos*, 553 U.S. 507, 516 (2008).

208 *United States v. Kozeny*, 493 F. Supp. 2d 693, 706 (S.D.N.Y. 2007), aff'd, 541 F.3d 166 (2d Cir. 2008) ('The elements of a money laundering offense do not include, or even implicate, the capacity to commit the underlying unlawful activity.').

209 18 U.S.C. § 1956(f).

© Law Business Research 2021

This express provision overcomes the presumption against extraterritoriality.[210]

A number of courts have addressed the requirement (applicable only in cases in which the defendant is not a US citizen) that 'the conduct occurs in part in the United States'.[211] This requirement does not mean that the defendant must have been physically present in the United States.[212] Courts have held that, irrespective of the defendant's physical presence, 'a transfer from a foreign account to an account in a US financial institution and a transfer from a US account to a foreign financial institution occur in part in the United States under 18 USC Section 1956(f)'.[213] Fewer cases have addressed whether Section 1956(f) is satisfied by a transfer from one foreign bank to another that passes through a correspondent or intermediate bank in the United States.[214] On this issue, results have been mixed.[215]

Because the MLCA applies extraterritorially and does not require proof that the defendant engaged (or had the capacity to engage) in specified unlawful activity, prosecutors may use the statute to charge individuals otherwise beyond the reach of US criminal law. For example, foreign officials who take bribes are not subject to FCPA liability. But foreign officials have been prosecuted

---

210 In *United States v. Ojedokun*, 2021 WL 4955239 (4th Cir. 26 Oct. 2021), the Fourth Circuit held that § 1956(f) 'overcomes the presumption against extraterritorial jurisdiction not only as applied to the substantive money laundering offenses, but also with respect to conspiracy offenses under § 1956(h).' Id. at *9.

211 18 U.S.C. § 1956(f)(1); see also *Ojedokun*, 2021 WL 4955239, at *11 (rejecting argument that defendant's conspiratorial conduct did not 'occur in part in the United States' and concluding that by 'making an agreement with at least one resident of the United States and engaging in a conspiracy extensively carried out in this country, he took part in a course of conduct relevant to the § 1956(h) charge that transpired within the United States, placing his actions squarely within the confines of § 1956(h)').

212 *United States v. Stein*, No. 93-cr-375, 1994 WL 285020, at *4–5 (E.D. La. 23 Jun. 1994).

213 *United States v. Firtash*, 392 F. Supp. 3d 872, 886 (N.D. Ill. 2019); see *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 93 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 23 April 2018) (collecting cases).

214 See *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d at 95 (characterising the issue as 'a question of first impression in this Court' that 'has not been considered widely').

215 Compare id. at 93–96 ('In this case, the United States alleges that Lazarenko and his associates transferred millions of dollars to and from accounts and between foreign bank accounts as [electronic funds transfers] that passed through US financial institutions. In the Court's view, this conduct is precisely what Congress intended to prevent in enacting the money laundering statutes – the use of US financial institutions as clearinghouses for criminal money laundering.'), and *United States v. Prevezon Holdings, Ltd.*, 251 F. Supp. 3d 684, 694 (S.D.N.Y. 10 May 2017) ('[T]he use of US correspondent banks to launder illegal proceeds qualifies as domestic conduct.'), with *United States v. Lloyds TSB Bank PLC*, 639 F. Supp. 2d 314, 324 n.4 (S.D.N.Y. 2009) (characterising a correspondent bank transfer as 'peripheral and transitory contact with the United States' that does not satisfy § 1956(f)); see also *Firtash*, 392 F. Supp. 3d 886–87 (avoiding the question).

© Law Business Research 2021

under the money laundering statute for engaging in transactions to promote or conceal FCPA violations they are incapable of committing.[216]

Power to obtain evidence located overseas 29.11

Demands by US prosecutors and regulators for individuals and entities to produce evidence located abroad can lead to conflicts with foreign law. As the DOJ has recognised:

> *Every nation enacts laws to protect its sovereignty and can react adversely to American law enforcement efforts to gather evidence within its borders without authorization. Such efforts can constitute a violation of that nation's sovereignty or criminal law.*[217]

To mitigate against the potential for such conflict, US policy requires prosecutors to attempt to obtain evidence located abroad through mutual legal assistance treaties (MLATs) rather than unilateral compulsory process, such as grand jury and administrative subpoenas. To do otherwise requires prosecutors to obtain written permission from the DOJ's Office of International Affairs.[218] The United States has entered into MLATs with around 70 countries around the world.[219] MLATs enable US prosecutors to deploy foreign law enforcement authorities to gather evidence for US investigations using the power of foreign law to compel production. While MLATs are powerful evidence-gathering tools, the process can be cumbersome and time-consuming, therefore, US law permits prosecutors to obtain orders suspending the running of the limitation period for crimes under investigation for up to three years during the pendency of any MLAT request.[220]

Outside the MLAT process, US prosecutors often utilise *Bank of Nova Scotia* subpoenas to obtain financial records located overseas by serving subpoenas on US branches of foreign financial institutions.[221] These subpoenas have been

216 See, e.g., *United States v. Duperval*, 777 F.3d 1324, 1328–31 (11th Cir. 2015) (former Haitian official found guilty of laundering the proceeds of 'schemes in which international companies gave him bribes in exchange for favors'); Plea Agreement 11–12, *United States v. Mikerin*, No. 14-cr-529-TDC (D. Md. 31 Aug. 2015) (former Russian official pleaded guilty to laundering proceeds of a bribery scheme).

217 DOJ, Justice Manual § 9-13.510.

218 Id. § 9-13.525

219 The United States has also entered into agreements that do not rise to the treaty level, mutual legal assistance agreements with China and the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States. In addition, the SEC has entered into memoranda of understanding that enable it to obtain evidence from foreign securities regulators. SEC, Cooperative Arrangements with Foreign Regulators, available at https://www.sec.gov/about/offices/oia/oia_cooparrangements.shtml.

220 18 U.S.C. § 3292.

221 *In re Grand Jury Proceeding*, 691 F.2d 1384 (11th Cir. 1982).

© Law Business Research 2021

upheld by US courts even when compliance would require the subpoena recipient to violate foreign law.[222] Such was the case in *In Re: Sealed Case*, in which the DC Court of Appeals upheld civil contempt findings against three Chinese banks that had been served with subpoenas to produce records located in China, the production of which they maintained would violate Chinese law.[223] Two of the banks had US branches and were served with grand jury subpoenas. The third bank did not have a US branch and was served pursuant to a Patriot Act subpoena that gives prosecutors 'special investigatory tools when it comes to US correspondent bank accounts'.[224] The DOJ did not attempt to first gather the evidence sought pursuant to the mutual legal assistance agreement with China, arguing that any such attempt would be futile.[225] After conducting a comity analysis, the Court agreed and found that US interests outweighed the Chinese interests at issue.[226] The Court affirmed the contempt orders against all three banks.[227]

On 1 January 2021, the US Congress passed the Anti-Money Laundering Act of 2020 (AMLA) as part of the National Defense Authorization Act of 2021. This legislation dramatically expanded the government's subpoena power with respect to foreign banks that maintain correspondent accounts in the United States. In particular, the AMLA granted the Department of the Treasury and the DOJ authority to subpoena such foreign banks for records relating to any account at the bank, 'including records maintained outside of the United States', as long as the records are the subject of a federal criminal investigation, civil forfeiture action or certain other types of investigations.[228] Section 6308 also prohibits the foreign bank's employees, agents and attorneys from notifying account holders about the existence or contents of the subpoena.[229]

29.12 Conclusion

US authorities continue to investigate and bring cases based on conduct that largely takes place outside the United States. Practitioners should carefully analyse the conduct at issue and the elements of the applicable statutes to determine whether the conduct is outside the reach of US law.

222 Id.

223 932 F.3d 915 (D.C. Cir. 2019).

224 Id. at 920; 31 U.S.C. § 5318(k)(3)(A).

225 932 F.3d at 936.

226 Id.

227 Id. at 940.

228 AMLA § 6308 (adding 31 U.S.C. § 5318(k)(3)(A)(i)). Prior to the enactment of the AMLA, the DOJ was authorised by Section 5318 of the Patriot Act to subpoena foreign banks for records maintained abroad, but only related to correspondent accounts in the United States.

229 AMLA § 6308 (adding 31 U.S.C. § 5318(k)(3)(C)).

© Law Business Research 2021

30

Individual Penalties and Third-Party Rights: The UK Perspective

Elizabeth Robertson, Vanessa McGoldrick and Jason Williamson[1]

Individuals: criminal liability 30.1

The Serious Fraud Office (SFO) has agreed to a total of twelve deferred prosecution agreements (DPAs)[2] with corporates since their introduction in February 2014.[3] Terms of a DPA will likely require the company to co-operate on an ongoing basis, which may include co-operation in the prosecution of individuals. However, to date, the SFO has not been successful in prosecuting

1 Elizabeth Robertson is a partner and Vanessa McGoldrick and Jason Williamson are associates at Skadden, Arps, Slate, Meagher & Flom (UK) LLP.

2 DPAs are only available to corporate organisations.

3 See *Standard Bank*, available at https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-DPA-with-standard-bank/; *Sarclad Ltd*, available at https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/; *Tesco*, available at https://www.sfo.gov.uk/2017/04/10/sfo-agrees-deferred-prosecution-agreement-with-tesco/; *Rolls-Royce*, available at https://www.sfo.gov.uk/cases/rolls-royce-plc/; *Serco Geografix*, available at https://www.sfo.gov.uk/2019/07/04/sfo-completes-dpa-with-serco-geografix-ltd/; *Güralp Systems Ltd*, available at https://www.sfo.gov.uk/2019/12/20/three-individuals-acquitted-as-sfo-confirms-dpa-with-guralp-systems-ltd/; *Airbus SE* available at https://www.sfo.gov.uk/2020/01/31/sfo-enters-into-e991m-deferred-prosecution-agreement-with-airbus-as-part-of-a-e3-6bn-global-resolution/; *G4S Care & Justice Services (UK) Limited*, available at https://www.sfo.gov.uk/2020/07/17/sfo-receives-final-approval-for-dpa-with-g4s-care-justice-services-uk-ltd/ accessed 13 November 2020; *Airline Services Ltd*, available at https://www.sfo.gov.uk/download/airline-services-limited-deferred-prosecution-agreement/; Amec Foster Wheeler Energy Limited, available at https://www.sfo.gov.uk/2021/07/02/sfo-enters-into-103m-dpa-with-amec-foster-wheeler-energy-limited-as-part-of-global-resolution-with-us-and-brazilian-authorities/; and separate DPAs with two unnamed companies for Bribery Act offences, available at https://www.sfo.gov.uk/2021/07/20/sfo-secures-two-dpas-with-companies-for-bribery-act-offences/.

© Law Business Research 2021

any individual involved in the conduct related to a DPA and has dropped a number of its larger investigations into individuals. Recently, two individuals, who had been charged in relation to conduct connected to the *Serco Geografix* DPA, were acquitted following evidence-disclosure errors by the SFO.[4]

Nevertheless, conviction and charging rate figures from the SFO's annual report for 2020–21 indicate that it remains the SFO's focus to pursue individuals involved in corporate misconduct. The 2020–2021 report confirms that four individual defendants were convicted, and 20 defendants, comprising both individuals and corporates, were charged in that period. [5] Some of the most recent DPAs support this view. Six months after announcing the *Airbus* DPA, the SFO charged Airbus subsidiary GPT Special Project Management Limited and three individuals with corruption offences between 2007 and 2012 in relation to a £2 billion contract for the Saudi military. The individuals charged included GPT's former managing director and finance officer.[6] Elsewhere, two months after announcing the *G4S* DPA, the SFO charged three former G4S executives with multiple fraud offences in connection with a scheme to defraud the Ministry of Justice between 2009 and 2012.[7] While not connected to a DPA, the SFO has also had success in securing the conviction of three former Unaoil executives,[8] and more recently a former SBM Offshore executive, for conspiring to make corrupt payments to secure lucrative oil contracts in Iraq.[9]

On 6 August 2019, the SFO published its Corporate Co-operation Guidance, which forms part of the SFO's Operational Handbook. The guidance seeks to formalise the approach adopted during previous DPAs and outlines what the SFO expects corporates seeking to co-operate to provide in respect of individuals.

On 23 October 2020, the SFO updated its Operational Handbook, publishing a new chapter on DPAs. The new guidance emphasises the protection of the identity of individuals connected to the company entering the DPA, noting that consideration must be given to the 'necessity for and impact of the identities of third parties being published'. The SFO also notes that consideration should be given as to whether identifying a third party would comply with the Data Protection Act 2018 and the European Convention on Human Rights. Although the new guidance does not prohibit naming individuals in

4 https://www.ft.com/content/769c8883-fdee-4251-a4c8-993b510a1b1b.

5 SFO annual report 2020-2021, 20 July 2021 (https://www.sfo.gov.uk/download/annual-report-and-accounts-2020-2021/), last accessed 1 September 2021.

6 https://www.sfo.gov.uk/cases/gpt-special-project-management-ltd/, 30 July 2020, last accessed 13 November 2020.

7 https://www.sfo.gov.uk/2020/09/08/sfo-charges-three-former-g4s-executives-with-fraud-against-taxpayer/, 8 September 2020, last accessed 1 September 2021.

8 https://www.sfo.gov.uk/2020/07/13/former-unaoil-executives-guilty-of-giving-corrupt-payments-for-oil-contracts-in-post-occupation-iraq/, last accessed 13 November 2020.

9 https://www.sfo.gov.uk/2021/02/24/fourth-executive-convicted-of-bribery-in-post-occupation-iraq/, 24 February 2021, last accessed 1 September 2021.

© Law Business Research 2021

a DPA, it is a change to the DPA Code of Practice, which stood silent on the matter.

Following the acquittal of a former chief executive of Barclays in 2019,[10] when the Court of Appeal held that the individual was not the directing mind of the bank, and the renewed debate following the Law Commission's consultation on corporate criminal liability,[11] there could be a move towards a broader offence of failure to prevent fraud, which could result in corporates having to provide information on the individuals involved in the alleged misconduct. The relatively recent changes in the test for 'dishonesty' in criminal law may encourage prosecutors to pursue individuals for offences involving dishonesty, such as fraud or theft.

Under the test for dishonesty in *R v. Ghosh*,[12] the jury was first asked to consider whether the defendant's acts were dishonest by the ordinary standards of reasonable honest people. If the answer to that question was 'yes', the jury would then consider whether the defendant must have realised that their conduct was dishonest by those standards. In the case of *Ivey v. Genting Casinos t/a Crockfords*,[13] the Supreme Court held that the second limb of the *Ghosh* test no longer applies. The defendant's conduct, in light of his or her (subjective) knowledge or belief of the facts, must be judged as honest or dishonest by the (objective) standards of ordinary decent people alone.[14] This change will make it more difficult for defendants to escape liability on the basis of their own moral compass and potentially easier for prosecutors to secure a conviction.

While DPAs in the United Kingdom are not available for individuals – and there is no indication that they will be any time soon – there is an increasing emphasis on incentivising individuals to enter an early plea. Section 75 of the Sentencing Act 2020 contains the statutory authority that compels the courts to consider a reduction in the sentence of an offender who has pleaded guilty to an offence. Subsection 2 obliges the court to take into account the stage in the proceedings at which the offender indicated an intention to plead guilty; and the circumstances in which this indication was given. The Reduction in Sentence for a Guilty Plea: Definitive Guideline (the Definitive Guideline) guides the courts in establishing an appropriate level of reduction for offenders.[15] Unless, on the facts, there is a sufficiently good reason for a lower amount, there is a presumption that for each of the following categories, the recommended

10 *R v. Varley and others* [2019] EWCA Crim 1074.

11 https://www.lawcom.gov.uk/law-commission-seek-views-on-corporate-criminal-liability/.

12 [1982] QB 1053.

13 [2017] UKSC 67; also confirmed in *R v. Alex Julian Pabon* [2018] EWCA Crim 420.

14 In the recent judgment by the Court of Appeal in *R v. David Barton and Rosemary Booth* [2020] EWCA Crim 575, the court held that the Supreme Court's *obiter* commentary in *Ivey* should be followed.

15 The Definitive Guideline applies regardless of when the offence was committed, but where the first hearing was held on or after 1 June 2017. Prior to this, the Sentencing Guidelines Council guideline applies.

© Law Business Research 2021

reduction will be given. If the offender pleads guilty, the sentence should be reduced as follows:

- at the first stage of proceedings, by a maximum of one-third;
- after the first stage, by a maximum of a one-quarter; or
- after the trial has begun, by a maximum of one-tenth.[16]

The Sentencing Act 2020 also contains several provisions that can benefit an offender who assists in the investigation or prosecution of a crime. For example, if an offender provides or offers assistance in the investigation or prosecution of others, the court in return may reduce the offender's sentence.[17]

30.1.1 Imprisonment

The maximum sentence for an individual convicted on indictment of an offence by virtue of section 1, 2 or 6 of the Bribery Act 2010 is 10 years' imprisonment.[18] Furthermore, where a corporate commits an offence under section 1, 2 or 6, if the offence is proved to have been committed with the consent or connivance of a senior officer (or person purporting to act in such a capacity), that officer or person can also be punished.[19] An individual tried and convicted summarily of any of the aforementioned offences is liable to a maximum prison sentence of 12 months. An individual convicted following summary trial will (if the offence merits more severe sanction) be committed to the Crown Court for sentence.[20]

In cases of financial crime, it is rare for defendants to be charged with only one count, and in the most serious cases a judge can order the sentences for each individual count of which a defendant has been convicted to run consecutively.

Whether a judge perceives a concurrent or consecutive sentence as appropriate on the facts will be decided by reference to the same factors that judges tend to consider when deciding on the severity of a sentence, such as whether

16 Where the guilty plea is entered during the trial, the reduction should normally be decreased further, even to zero.

17 Sentencing Act 2020, s.74. See also ibid., s.388: A defendant, already serving a prison sentence, who provides or offers assistance in this regard could also benefit by having a sentence reviewed

18 See Bribery Act 2010, s.11. An individual cannot be convicted of an offence under s.7 of the Bribery Act because the offence refers only to a 'commercial organisation' for which the only sentence available is an unlimited fine.

19 See ibid., s.14.

20 The maximum sentence for individuals under the Bribery Act 2010 is identical for any of the fraud offences both at common law and under the Fraud Act 2006 but is far greater (up to a maximum of 14 years' imprisonment) for any of the substantive money laundering offences pursuant to the Proceeds of Crime Act 2002 (POCA), ss.327 to 329. Furthermore, an individual convicted of the tipping- off offence under POCA, s.333A is liable to a maximum of two years' imprisonment or a fine, or both.

© Law Business Research 2021

the defendant has any previous convictions, the magnitude of the offence[21] or where it can be established that the defendant failed to respond to warnings about his or her behaviour.

Despite the continued prominence of financial crime cases in the media and the apparent fervour of prosecutors and courts to ensure that convicted individuals receive long custodial sentences, suspended sentences may well be considered appropriate in some cases. In *R v. Dougall*,[22] an employee heading a company's corrupt Greek practice who pleaded guilty to conspiracy to corrupt, and who was a co-operating defendant under section 73 of the Serious Organised Crime and Police Act 2005,[23] had his 12-month custodial sentence suspended on appeal.[24] This case also demonstrates the risks individuals face when conduct spans multiple jurisdictions and no settlement or amount of co-operation provides an absolute guarantee against further proceedings being pursued in any jurisdiction.

See Chapter 17 on individuals in cross-border proceedings

See Chapter 23 on negotiating global settlements

The Attorney General's Guidelines on Plea Discussions in Cases of Serious or Complex Fraud (Attorney General's Guidelines) set out a process by which a prosecutor may discuss an allegation of serious or complex fraud with a suspect.[25] The implementation of the Attorney General's Guidelines, with the support of the judiciary and prosecuting authorities, has garnered a quasi-plea discussion system that can be advantageous to defendants. Although the Attorney General's Guidelines do not make any provision for a defendant to receive a greater discount on the sentence than is available for simply entering a guilty plea (as set out above), in a case brought by the FCA's predecessor, the Financial Services Authority (FSA),[26] against Paul Milsom, a senior equities trader, for disclosing inside information between October 2008 and March 2010, Judge Pegden QC indicated, in passing sentence on 18 March 2013 at Southwark Crown Court, that he had given Mr Milsom full credit for pleading guilty

21 In the Fraud, Bribery and Money Laundering Offences Definitive Guideline, it expressly states that: 'Consecutive sentences for multiple offences may be appropriate where large sums are involved.' https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, at p. 10 (last accessed 13 November 2020).

22 [2010] EWCA Crim 1048.

23 Since 1 December 2020, sentence reductions for co-operating defendants are governed by the Sentencing Act 2020, s.74. Such reductions previously fell under the Serious Organised Crime and Police Act 2005 (SOCPA), s.73.

24 The Court of Appeal held that 'where the appropriate sentence for a defendant whose level of criminality, and features of mitigation, combined with a guilty plea, and full co-operation with the authorities investigating a major crime involving fraud or corruption, with all the consequent burdens of complying with his part of the SOCPA agreement, would be 12 months' imprisonment or less, the argument that the sentence should be suspended is very powerful'. [2010] EWCA Crim 1048, at para. 36.

25 The Attorney General's Guidelines came into force on 5 May 2009.

26 As of 3 April 2013, the FSA became two separate regulatory bodies – the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

© Law Business Research 2021

at the earliest opportunity (i.e., a discount of one-third) and extra credit for entering into a plea agreement with the FSA.[27] The sentencing remarks of Judge Pegden QC convey the 'clearest articulation to date that an individual can reasonably expect to receive in excess of one third discount on sentence in circumstances where he enters into early plea discussions with a prosecutor'.[28]

30.1.2 Fines

Fines for individual perpetrators of financial crime can be unlimited and are handed down either separately or in conjunction with a custodial sentence. Sections 124 to 126 of the Sentencing Act 2020 regulate the fixing of fines in criminal cases. Those sections require that any fine imposed must reflect the seriousness of the offence and require the court to take into account the financial circumstances of the offender.

30.1.3 Unexplained wealth orders

The Criminal Finances Act 2017 (CFA 2017) came into force on 30 September 2017 and created a new High Court power to make an unexplained wealth order (UWO), which can require a person who is suspected of involvement in, or association with, serious criminality or who is a politically exposed person (PEP) to explain the origin of assets that appear to be disproportionate to their known income.[29] A failure to provide a response will give rise to a presumption that the property is recoverable, in order to assist any subsequent civil recovery action. UWOs are intended to alleviate the burden on enforcement authorities and come with wide-ranging powers to gather evidence in other jurisdictions and potentially support parallel enforcement actions. The powers to make UWOs under the CFA 2017 commenced on 31 January 2018, with the National Crime Agency (NCA) obtaining at least 15[30] UWOs since commencement.

The CFA 2017 enables a number of UK regulators and enforcement agencies, namely the SFO, the NCA, HM Revenue and Customs, the FCA and the Director of Public Prosecutions, to apply to the High Court for a UWO, regardless of whether civil or criminal proceedings have been initiated

27 https://webarchive.nationalarchives.gov.uk/20130402175500/http://www.fsa.gov.uk/library/communication/pr/2013/022.shtml, last accessed 13 November 2020.

28 Chris Dyke, The Benefits of Early Plea Discussions, https://www.corkerbinning.com/corker-binning-solicitor-writes-about-the-benefits-of-early-plea-discussions-in-crimeline/ (last accessed 13 November 2020).

29 Under the Criminal Finances Act 2017, Part 1 ss.1–9, which amends POCA s.362.

30 The NCA's National Strategic Assessment of Serious and Organised Crime stated that it had obtained 15 UWOs over property worth an estimated £143 million. Its publication was made prior to the discharge of three UWOs on 8 April 2020 in *National Crime Agency v. Baker & Ors* [2020] EWHC 822 (Admin). Recognising the impact the judgment would have in subsequent UWO applications, the NCA immediately sought to appeal the decision, but the Court of Appeal refused the application.

© Law Business Research 2021

against the respondent to the order or whether the respondent is located in the United Kingdom or another jurisdiction.[31]

There must be reasonable cause to believe that the respondent holds the property and that the value of the property is greater than £50,000. There must also be reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income would have been insufficient for the purposes of enabling the respondent to obtain the property. Respondents must also either be (1) a PEP or (2) someone for whom there are reasonable grounds for suspecting that they have been involved in serious crime. Under the CFA 2017, a person is considered to be involved in serious crime in the United Kingdom or another jurisdiction if the person would be so involved for the purposes of Part 1 of the Serious Crime Act 2007.[32]

The first UWO, obtained in February 2018, was made against two properties valued at approximately £22 million, connected to Mrs Zamira Hajiyeva, the wife of Mr Jahangir Hajiyev, a former banker imprisoned for fraud and embezzlement in Azerbaijan. Mrs Hajiyvera challenged the orders in the High Court on a number of grounds, including that her husband had been incorrectly classified as a PEP. However, the court dismissed these challenges, finding that Mr Hajiyev was a PEP from a non-EEA country against whom a UWO could be granted, and that as his wife, Mrs Hajiyeva was herself also a PEP.[33] Having been unsuccessful in the High Court, Mrs Hajiyeva applied to the Court of Appeal on the basis that the court had *inter alia* erred in relying on Mr Hajiyev's conviction in Azerbaijan for fraud and corruption offences as evidence that his lawful income was insufficient to purchase the properties.[34] The Court of Appeal dismissed the appeal, agreeing with the High Court's reasoning. The consistent approach taken by both the High Court and the Court of Appeal demonstrates that a respondent seeking to discharge a UWO on the basis that the 'income test' is not satisfied will have to demonstrate evidence of lawful income sufficient to have purchased the property in question.

A second UWO against a respondent considered to be involved in serious crime followed on 24 July 2019 against six properties worth around £3.2 million

31 As of August 2021 and according to publicly available information, only the NCA has applied for UWOs.

32 This widens the category of potential respondents significantly to include persons who (1) have committed a serious offence, (2) have facilitated the commission of an offence or (3) conducted themselves in a way that was likely to facilitate the commission by themselves – or another person – of a serious offence, whether or not the offence was committed. The Criminal Finances Act 2017 (CFA 2017) widens the category of respondents even further to include anyone who is connected with a person who is or has been involved in serious crime, whether in the United Kingdom or in another jurisdiction.

33 *National Crime Agency v. Mrs A* [2018] EWHC 2534 (Admin).

34 *National Crime Agency v. Hajiyeva* [2020] EWCA Civ 108. It was also submitted that the High Court had erred in applying the statutory test to identify a PEP and that the UWO itself conflicted with the rules against spousal privilege and self-incrimination.

© Law Business Research 2021

in total belonging to a woman believed to be associated with criminals involved in paramilitary activity and cigarette smuggling.[35]

Interim freezing orders can also be granted by the High Court with each UWO, under section 362J POCA, meaning that the assets subject to the UWOs cannot be sold, transferred or dissipated for the duration of the order.

Respondents are required by a UWO to provide certain information about the specified property, including the nature and extent of the respondent's interest, how it was obtained and any other information specified in the order. Aside from contempt of court proceedings, the failure to respond to a UWO creates a presumption that the property is recoverable in civil proceedings, which reduces the burden imposed on enforcement authorities under the current POCA regime, to prove that property derives from criminal conduct or constitutes the proceeds of crime. Section 362S of POCA provides that when a UWO is issued, where the enforcement authority believes that the property is outside the United Kingdom, it may send a request for assistance in relation to the property to the Secretary of State, who in turn may forward the request to the government of the receiving country.

Where a respondent complies or purports to comply, the enforcement authority must determine, within 60 days starting with the date of compliance, what enforcement or investigatory proceedings, if any, it considers ought to be taken in relation to the property.

POCA also provides that a criminal offence is committed if a respondent gives a false or misleading statement in response to a UWO, with a maximum penalty of two years' imprisonment.[36] The CFA 2017 amends POCA so that the FCA and HMRC have civil recovery powers to recover property in cases where there has not been a conviction but where it can be shown on the balance of probabilities that property has been obtained by unlawful conduct. Such proceedings would be brought in the High Court to recover criminal property without the need for the owner of the property to be convicted of a criminal offence.[37] The NCA has sought to make use of this new tool. On 14 August 2019, it announced that account freezing orders (AFOs) had been obtained at Westminster magistrates' court over eight bank accounts holding more than £100 million.[38]

30.1.4 Confiscation orders

It is becoming more common for courts to address the confiscation of the assets of a convicted individual, especially when the court is satisfied that the

35 https://www.nationalcrimeagency.gov.uk/news/nca-secures-unexplained-wealth-order-against-properties-owned-by-a-northern-irish-woman (last accessed 13 November 2020).

36 POCA, s.362E.

37 This is a lower threshold than that required for restraint proceedings under POCA, where a criminal investigation or proceedings must have been commenced.

38 https://www.nationalcrimeagency.gov.uk/news/100m-account-freezing-orders-are-largest-granted-to-nca (last accessed 13 November 2020).

© Law Business Research 2021

defendant was said to be living a 'criminal lifestyle'.[39] Furthermore, Step 6 of the Sentencing Council Guidelines on Fraud, Bribery and Money Laundering Offences states that the court must proceed with a view to making a confiscation order if it is asked to do so by the prosecutor or if the court believes it is appropriate to do so.[40] The FCA secured £1.9 million in confiscation orders on 11 May 2018, as part of Operation Tabernula,[41] and £2.2 million in confiscation orders in May 2017, as part of Operation Cotton.[42]

Confiscation orders, which are debts to the Crown, are available only after a defendant has been convicted. Where a confiscation order is not paid, the defendant will serve a period of imprisonment in default. This mechanism is highlighted in the case of Jolan Saunders, whose default prison sentence of 3,236 days (just under nine years) was activated after he failed to pay a confiscation order of £5,262,301.03, despite the SFO showing evidence of £4.5 million in hidden assets emanating from his fraud.[43]

The Supreme Court also recently clarified the position regarding the reduction of default sentences for partial repayment of sums ordered under a confiscation order. In *R (on the application of Gibson) v. Secretary of State for Justice*,[44] the Supreme Court held that the calculation of reductions in default terms should not take into consideration accrued interest. The ruling confirms that there is a continued incentive for individuals subject to confiscation orders to continue making contributions even after a default sentence has been triggered.

Confiscation orders derive from section 6 of POCA and are intended to deprive the defendant of the benefit of any proceeds of his or her crimes; they are not, however, intended to act as a fine or further punishment. They do not always involve the sequestration of the defendant's personal property. Instead, they usually entail the payment of a sum of money: 'Where, however, a criminal has benefited financially from crime but no longer possesses the specific fruits of his crime, he will be deprived of assets of equivalent value, if he has them.'[45]

---

39 Pursuant to POCA, s.75, '(1) a defendant has a criminal lifestyle if (and only if) the following condition is satisfied. (2) The condition is that the offence (or any of the offences) concerned satisfies any of these tests – (a) it is specified in Schedule 2; (b) it constitutes conduct forming part of a course of criminal activity; or (c) it is an offence committed over a period of at least six months and the defendant has benefited from the conduct which constitutes the offence'.

40 https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, accessed 13 November 2020.

41 https://www.fca.org.uk/news/press-releases/fca-secures-1-6m-confiscation-order-against-richard-baldwin (last accessed 23 November 2020).

42 https://www.fca.org.uk/news/press-releases/fca-secures-confiscation-orders-totalling-1-69-million-against-convicted-insider-dealers; https://www.fca.org.uk/news/press-releases/fca-secures-eight-confiscation-orders-totalling-almost-22-million (last accessed 13 November 2020).

43 https://www.sfo.gov.uk/2021/08/02/london-fraudster-jailed-for-failing-to-pay-confiscation-order/ (last accessed 22 August 2021).

44 [2018] UKSC 2.

45 *R v. May* [2008] UKHL 28, at para. 9.

© Law Business Research 2021

In accordance with the decision in *R v. Waya*,[46] prosecutors should ensure that the confiscation is proportionate, which entails an assessment of the ability of the defendant to pay the order in full.

The Attorney General's Guidelines are silent as to confiscation orders – they provide no framework to regulate the discussions and agreement of confiscation orders as part of plea discussions. Should the prosecution and the defendant reach any form of agreement in relation to a confiscation order, that agreement would not bind a court. In Mr Milsom's case, however, the judge agreed to make a confiscation order at the sentencing hearing in the value of his personal benefit from his offending, which had been agreed between the prosecution and the defence within the basis of the plea and joint sentencing submission. This suggests that prosecutors could be willing to negotiate the terms of a confiscation order as part of a plea negotiation, and that the courts may be willing to accept the joint submission that 'provid[es] a defendant with greater certainty and control over his financial liabilities'.[47]

The burden of proof in criminal confiscation orders rests with the defendant, who must show, on the balance of probabilities, that his or her assets are not derived from criminal conduct.

Where it is reasonably foreseeable that a court will make a confiscation order, the prosecution may take steps in the High Court to ensure that the defendant's assets will remain available to meet the terms of the order. Such steps include, *inter alia*, an order requiring the defendant to disclose where assets are kept, an order appointing a receiver and an order restraining assets.[48]

30.1.5 Compensation orders

Like a confiscation order, a compensation order is an ancillary court order and is designed to compensate a victim for personal injury or any loss or damage that may have resulted from the offence committed by the defendant and is made in addition, or instead of, other sentencing options under section 130 of the Powers of Criminal Courts (Sentencing) Act 2000. The Sentencing Council Guidelines on Fraud, Bribery and Money Laundering Offences also provide that, under Step 6, the court must proceed with a view to making a confiscation order, if it is asked to do so by the prosecutor, or if the court believes it is appropriate to do so.[49]

46 [2012] UKSC 51.

47 Chris Dyke, 'The Benefits of Early Plea Discussions', https://www.corkerbinning.com/corker-binning-solicitor-writes-about-the-benefits-of-early-plea-discussions-in-crimeline/ (last accessed 13 November 2020).

48 See Senior Courts Act 1981, s.37(1).

49 https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf (last accessed 13 November 2020).

© Law Business Research 2021

In both a magistrates' court[50] and the Crown Court, the amount that can be awarded as compensation is now unlimited but is restricted to an amount that can feasibly be paid by the defendant. The court must have regard to the evidence of the defendant's financial means when deciding the level of compensation to award the victim and must prioritise the payment of compensation over any other financial penalty.

Disqualification orders 30.1.6

Directors of companies are fiduciaries and there is consequently a high level of probity expected of them by the law. It is therefore expected that '[t]hose who are involved in bribery, whether as individuals or as part of their role as directors, are very likely to be disqualified from acting as a director for a lengthy period of time'.[51]

Directors disqualification orders (DDOs) are designed to help protect creditors and the public from those individuals who may act dishonestly and can bar a person from acting as a director of any UK company for up to 15 years. DDOs can be made where the defendant director of a company has been convicted of an indictable offence which, by virtue of the decision in *R v. Creggy*,[52] must have some relevant factual connection with the management of the company.

See Chapters 25 on fines, disgorgement, etc. and 42 on directors' duties

Costs 30.1.7

As in all criminal cases, cost orders are usually made against a convicted defendant, who will be required to pay the prosecution's costs as well as any court fees that materialise during the criminal proceedings.[53]

Individuals: regulatory liability 30.2

The FCA has continued the FSA's legacy of adopting a robust enforcement stance, underpinned by its 'credible deterrence' strategy. In furtherance of its policy of 'credible deterrence', the FSA had signalled a willingness to pursue criminal actions through the courts and to seek custodial sentences. For the FCA, the pursuit of criminal prosecutions, where appropriate, remains high on its agenda, particularly for market misconduct offences. This is supported by the

50 Before 11 December 2013, the amount that a magistrate could award as part of a compensation order was £5,000, but, by virtue of the Powers of Criminal Courts Sentencing Act 2000, s.131, this limit has been removed.

51 Eoin O'Shea, *The Bribery Act 2010, A Practical Guide*, Jordans, at p. 238.

52 [2008] EWCA Crim 394.

53 The legislative authority enabling a court to award costs in criminal proceedings is primarily contained in Part II of the Prosecution of Offences Act 1985 (ss.16 to 19B); the Access to Justice Act 1999; the Legal Aid, Sentencing and Punishment of Offenders Act 2012 (in relation to funded clients); and in regulations that have since been made pursuant to these statutes, including the Costs in Criminal Cases (General) Regulations 1986, as amended.

© Law Business Research 2021

FCA's Annual Business Plan for 2021/22, which illustrates that tackling financial crime, including fraud, remains a priority. The UK government's Economic Crime Plan 2019-22 also lists strengthening the capabilities of law enforcement as one of its strategic priorities, 'to detect, deter and disrupt economic crime'.[54] The FCA has introduced further changes to the Senior Managers and Certification Regime, which came into force on 9 December 2019, extending the regime to FCA solo-regulated firms[55] to make senior managers more responsible and accountable for their actions.[56]

See Chapters 25 on fines, disgorgement, etc. and 42 on directors' duties

Under the Financial Services and Markets Act 2000 (FSMA) as amended by the Financial Services Act 2012, the FCA has many tools at its disposal to punish non-criminal offences and breaches. This includes the issuing of public censures or statements, and imposing unlimited financial penalties. A number of other sanctions are available to the FCA.[57]

Chapter 6 of the FCA's Decision Procedure and Penalties manual (DEPP) contains the FCA's statement of policy in relation to the imposition and amount of penalties under FSMA.[58] DEPP 6A sets out its policy in relation to imposing suspensions or restrictions on firms and on approved persons. Chapter 7 of the FCA's Enforcement Guide sets out specific guidance on the FCA's powers in relation to financial penalties and public censures. Further, in April 2017, the FCA published an Enforcement Information Guide, which should be read in conjunction with DEPP and the Enforcement Guide.

See Chapter 25 on fines, disgorgement, etc.

30.3 Other issues: UK third-party rights

Section 393 FSMA gives third parties certain rights in relation to warning and decision notices given to another person in respect of whom the FCA is taking regulatory action. Where a warning notice has been given, section 393(1) provides that a third party prejudicially identified in the notice must be given a copy and a reasonable period to make representations on it.[59] No equivalent

54 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf.

55 'Solo-regulated firms' are firms that are regulated exclusively by the FCA rather than dually regulated by the FCA and Prudential Regulatory Authority. The regime commenced for benchmark administrators on 7 December 2020 to allow the FCA to carry out a dedicated consultation for benchmark administrators before making final rules for the sector.

56 https://www.fca.org.uk/firms/senior-managers-certification-regime/banking; https://www.fca.org.uk/publication/policy/ps18-14.pdf, last accessed 13 November 2020.

57 Other sanctions available to the FCA include varying or cancelling a firm's permission under the FSMA, Part 4A; intervening against an incoming EEA or EU Treaty firm; suspending or restricting a firm's Part 4A permissions; suspending or restricting the approval given to an approved person; prohibiting an individual from performing regulated functions; withdrawing the approval of an approved person; imposing a penalty on a person who has performed a controlled function without approval; and issuing a private warning.

58 In August 2018, the FCA issued a new version of the DEPP.

59 Unless he or she has been given a separate warning notice in relation to the same matter.

© Law Business Research 2021

regime exists in the criminal sphere, where the DPA process (which involves the agreed statement of facts detailing the conduct of individuals) enables individuals to respond prior to the DPA being entered into.

Section 393(4) gives third-party rights in relation to a decision notice. It provides that a third party prejudicially identified in the notice must be given a copy of it and a reasonable period to make representations on it. Section 393(11) provides that a person who alleges that a copy of the notice should have been given to him or her may refer that alleged failure to the Upper Tribunal.[60]

The scope of the rights conferred by section 393(4) was reconsidered in *Macris v. FCA*.[61] On 22 March 2017, the majority of the Supreme Court stated that someone is identified in a notice if 'he is identified by name or by a synonym for him, such as his office or job title'. Such a synonym would need to be 'apparent from the notice itself that it could apply to only one person and that person must be identifiable from information which is either in the notice or publicly available elsewhere'. Information from other sources can only be used to interpret the language of the FCA's notice, rather than to supplement it, and must be easily ascertainable.

60 In April 2010, the Financial Services and Market Tribunal, established by the FSMA, s.132 as an independent judicial body to hear decision notices issued by the FSA, was abolished and its functions transferred to the Upper Tribunal.

61 [2015] EWCA Civ 490; [2017] UKSC 19.

© Law Business Research 2021

31

Individual Penalties and Third-Party Rights: The US Perspective

Todd Blanche and Cheryl Risell[1]

31.1 Prosecutorial discretion

31.1.1 Generally

In the United States, prosecutors usually have discretion in deciding whether to investigate and charge an individual with an offence.[2] As a threshold matter, a prosecutor may bring charges if there is probable cause to believe that the accused has committed a crime.[3] Prosecutors also have discretion as to how

1 Todd Blanche is a partner and Cheryl Risell is an associate at Cadwalader, Wickersham & Taft LLP.

2 See *United States v. Armstrong*, 517 U.S. 456, 464 (1996) (holding that the constitutional separation of powers requires broad prosecutorial discretion); *Young v. United States ex. Rel. Vuitton et Fils S.A.*, 481 U.S. 787, 807 (1987) (holding that prosecutors have discretion to decide which persons should be the target of an investigation); *Wayte v. United States*, 470 U.S. 598, 607 (1985) (finding that courts are ill-equipped to evaluate the strength of a prosecutor's case, a case's deterrent value, and the government's enforcement priorities). See also American Bar Association, Criminal Justice Standards for the Prosecution Function (4th ed. 2018), Standard 3-4.2 (Decisions to Charge are the Prosecutor's), https://www.americanbar.org/groups/criminal_justice/standards/ProsecutionFunctionFourthEdition/.

3 See *Bordenkircher v. Hayes*, 434 U.S. 357, 364 (1978) (holding that, if a prosecutor has probable cause to believe that the accused committed an offence, the decisions whether to prosecute and what charges to file rest entirely within his discretion). See also *Rinaldi v. United States*, 434 U.S. 22, 29–30 (1977) (*per curiam*) (holding that the prosecutor has discretion to dismiss charges unless dismissal would be contrary to the public interest).

© Law Business Research 2021

to charge a specific offence,[4] when to bring charges[5] and whether to negotiate a plea agreement.[6] Courts will typically not interfere with charging decisions absent a showing of selective prosecution[7] or vindictive prosecution.[8]

Principles of Federal Prosecution 31.1.2

The Department of Justice (DOJ) issues guidance to federal prosecutors to assist them in exercising their discretion appropriately when making investigation and charging decisions.

The DOJ's Principles of Federal Prosecution – issued as part of the Justice Manual (JM) – provide federal prosecutors with a framework for applying their prosecutorial discretion to 'promote the reasoned exercise of prosecutorial authority and contribute to the fair, evenhanded administration of the Federal criminal laws'.[9] The Principles provide that if a prosecutor concludes that there is probable cause to believe that a person has committed a federal offence within the prosecutor's jurisdiction, the prosecutor should consider whether to:

- request or conduct further investigation;
- commence or recommend prosecution;
- decline prosecution and refer the matter for prosecutorial consideration in another jurisdiction;
- decline prosecution and commence or recommend pretrial diversion or other non-criminal disposition; or
- decline prosecution without taking other action.[10]

A prosecutor should commence or recommend federal prosecution if he or she believes that the person's conduct constitutes a federal offence, and that the admissible evidence will probably be sufficient to obtain and sustain a conviction, unless (1) the prosecution would serve no substantial federal interest, (2) the person is subject to effective prosecution in another jurisdiction or (3) there exists an adequate non-criminal alternative to prosecution.[11]

4 See *United States v. Batchelder*, 442 U.S. 114, 123–25 (1979) (holding that it is proper for prosecutors to bring charges under any statute unless brought for a discriminatory purpose).

5 See *United States v. Lovasco*, 431 U.S. 783, 795–96 (1977) (holding that an 18-month delay in bringing charges did not violate the defendant's due process rights).

6 See *Weatherford v. Bursey*, 429 U.S. 545, 561 (1977) (holding there is no constitutional right to plea bargain).

7 See *Yick Wo v. Hopkins*, 118 U.S. 356, 373–74 (1886) (selective prosecution of Chinese laundry owners but not similarly situated non-Chinese laundry owners).

8 See *Blackledge v. Perry*, 417 U.S. 21, 28-29 (1974) (prosecution of a defendant for a more serious charge in a new trial following a successful appeal of his original conviction).

9 US Dep't of Justice (DOJ), Justice Manual (JM), Principles of Federal Prosecution, § 9-27.000 et seq., https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution.

10 Id., at § 9-27.200 (Initiating and Declining Prosecution – Probable Cause Requirement).

11 Id., at § 9-27.220 (Grounds for Commencing or Declining Prosecution).

© Law Business Research 2021

In determining whether a prosecution 'would serve a substantial federal interest', the Principles of Federal Prosecution advise prosecutors to weigh all relevant considerations, including:

- federal law enforcement priorities, including any federal law enforcement initiatives or operations aimed at accomplishing those priorities;
- the nature and seriousness of the offence;
- the deterrent effect of prosecution;
- the person's culpability in connection with the offence;
- the person's history with respect to criminal activity;
- the person's willingness to co-operate in the investigation or prosecution of others;
- the person's circumstances;
- the interests of any victims; and
- the probable sentence or other consequences if the person is convicted.[12]

31.1.3 DOJ enforcement priorities and policies

Every year, the Attorney General communicates the DOJ's national enforcement priorities, which have ranged from a focus on drug prosecutions during the influx of crack cocaine in the 1980s, to national security and counterterrorism following the attacks of 11 September 2001, and to prosecuting mortgage and financial fraud as the result of the Wall Street credit crisis of 2008. In the wake of the covid-19 pandemic, the DOJ's leadership has emphasised swift investigations of price gouging for needed drugs or personal protection equipment and created national task forces to address that.[13]

In addition, the DOJ encouraged immediate prosecutions and arrests of individuals alleged to have defrauded the Small Business Administration's Payroll Protection Program (PPP), which provided direct and immediate loans to qualified businesses to enable them to keep employees on the payroll.[14] The

12 Id., at § 9-27.230 (Initiating and Declining Charges – Substantial Federal Interest).

13 On 19 March 2020, the US Attorney General William P Barr announced a coordinated nationwide response to 'detect, deter and punish' crime relating to covid-19, creating a national hotline to report fraud and directing all United States Attorney's Offices to establish a Coronavirus Director for each office. Office of the Deputy Attorney General, US Department of Justice, Coordinated Nationwide Response to Detect, Deter, and Punish Crime Relating to the National Emergency Caused by COVID-19 (19 March 2020), https://www.justice.gov/file/1268521/download; Office of the Attorney General, US Department of Justice, Memorandum for All Heads of Department Components and Law Enforcement Agencies and All United States Attorneys (24 March 2020), https://www.justice.gov/file/1262776/download.

14 See, e.g., DOJ press release, 'Department of Justice FY 2021 Budget Request' (10 Feb. 2020), https://www.justice.gov/opa/pr/department-justice-fy-2021-budget-request-0 (listing combating violent crime, countering incidents of mass violence, the opioid crisis and combating transnational criminal organisations known for supplying illicit substances to the United States, implementation of the First Step Act, immigration law enforcement, national

© Law Business Research 2021

DOJ has already brought cases against persons for covid-19 related fraud, such as fraudulent PPP loan applications, Economic Injury Disaster Loan programs and Unemployment Insurance programs. By March 2021, the Justice Department had already publicly charged 474 defendants with criminal offences based on covid-19 fraud schemes.[15] For example, three men in Florida pleaded guilty to conspiring to launder proceeds obtained from business email compromise schemes and fraudulently obtained covid-19 relief loans.[16] A businesswoman in Georgia pleaded guilty to bank fraud of more than $6 million in connection with the PPP.[17] In the coming years, enforcement for fraud and other illegal activity related to covid-19 is likely to be a priority for the Justice Department. Further, the DOJ periodically issues policy guidance that has an impact on prosecutorial discretion, frequently corresponding to changes in DOJ leadership. For example, on 10 May 2017, then-Attorney General Jeff Sessions issued a memorandum to all federal prosecutors entitled 'Department Charging and Sentencing Policy', which directed that 'prosecutors should charge and pursue the most serious, readily provable offence'.[18] In addition, the memorandum directed prosecutors to disclose to the court 'all facts that impact the sentencing guidelines or mandatory minimum sentences'.[19] By this memorandum, the Attorney General modified charging policies then in effect, limiting prosecutors' discretion in making charging decisions and sentencing recommendations and requiring any exceptions to be approved by the respective US Attorney.[20] In March 2020, the Justice Department and the Federal Trade Commission announced expedited antitrust procedures and guidance for coronavirus public health efforts, providing direction for collaborations of businesses working to protect the health and safety of Americans during the covid-19 pandemic. The agencies stressed they would not hesitate to hold accountable those who try to use the pandemic to engage in antitrust violations, and would criminally prosecute conduct such as price-fixing, bid rigging

security and cyber and safety for law enforcement personnel as among the DOJ's federal law enforcement priorities for Fiscal Year 2021).

15 DOJ press release, 'Justice Department Takes Action Against COVID-19 Fraud' (26 Mar. 2021), https://www.justice.gov/opa/pr/justice-department-takes-action-against-covid-19-fraud.

16 DOJ press release, 'Three South Florida Men Guilty of Conspiring to Launder Fraudulently Obtained Covid-19 Relief Money and Proceeds from Business Email Compromise Schemes' (2 Sep. 2021), https://www.justice.gov/usao-sdfl/pr/three-south-florida-men-guilty-conspiring-launder-fraudulently-obtained-covid-19-relief.

17 DOJ press release, 'Roswell businesswoman pleads guilty to bank fraud in connection with the Paycheck Protection Program' (18 August 2021), https://www.justice.gov/usao-ndga/pr/roswell-businesswoman-pleads-guilty-bank-fraud-connection-paycheck-protection-program.

18 Office of the Attorney General, DOJ, Department Charging and Sentencing Policy (10 May 2017), https://www.justice.gov/opa/press-release/file/965896/download.

19 Id.

20 In February 2018, the DOJ amended JM § 9-27.300 (Selecting Charges – Charging Most Serious Offences) to incorporate the May 2017 Sessions Memo stating that federal prosecutors must pursue the most serious offences that carry the most substantial Guidelines sentence.

© Law Business Research 2021

or market allocation.[21] In May 2021, Attorney General Merrick Garland announced an effort by the Justice Department to reduce violent crime. [22] The strategy is three-pronged and includes (1) the establishment of four principles[23] to guide violent crime reduction, (2) enhancement of the Project Safe Neighborhoods programme to align with the Justice Department's guiding principles to improve community engagement and strategic enforcement plans, and (3) a directive to each US Attorney's Office to work with its state, local, federal, tribal and community partners to address spikes in violent crime.[24] The use of these memoranda and announcements by the DOJ leadership is another mechanism by which policy changes are put into effect.

In a keynote address on 28 October 2021,[25] Deputy Attorney General Lisa O Monaco emphasised the DOJ's priority of white-collar crime enforcement and announcing new three new DOJ policies regarding corporate criminal investigations. Setting the tone for these policies, Monaco emphasised that federal prosecutors should 'be bold in holding accountable' white-collar criminal defendants, urging that as long as prosecutors believe a defendant's conduct constitutes an offence and admissible evidence can sustain a conviction, 'the fear of losing should not deter' prosecutors from bringing charges. Towards that goal, Monaco announced the DOJ's new policy that co-operation credit requires full disclosure of all individuals involved in wrongdoing. In the context of corporate criminal enforcement, Monaco stressed that prosecutors 'first need to know the cast of characters involved in any misconduct'. As a result, she announced that companies may only be eligible for co-operation credit if they 'identify all individuals involved in the misconduct, regardless of their position, status or seniority'. Monaco drew a sharp contrast between this new policy of

21 DOJ press release, 'The Justice Department and the Federal Trade Commission Announce Expedited Antitrust Procedure and Guidance for Coronavirus Public Health Efforts' (24 March 2020), https://www.justice.gov/opa/pr/justice-department-and-federal-trade-commission-announce-expedited-antitrust-procedure-and.

22 DOJ press release, 'Attorney General Merrick B. Garland Announces New Effort to Reduce Violent Crime' (26 May 2021), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-new-effort-reduce-violent-crime; Office of the Deputy Attorney General, US Department of Justice, Comprehensive Strategy for Reducing Violent Crime (26 May 2021), https://www.justice.gov/dag/page/file/1397921/download.

23 The four principles are (1) build trust and earn legitimacy, (2) invest in prevention and intervention programmes, (3) target enforcement efforts and priorities, and (4) measure results. See DOJ press release, 'Attorney General Merrick B. Garland Announces New Effort to Reduce Violent Crime' (26 May 2021), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-new-effort-reduce-violent-crime.

24 DOJ press release, 'Attorney General Merrick B. Garland Announces New Effort to Reduce Violent Crime' (see supra note 22); Office of the Deputy Attorney General, US Department of Justice, Comprehensive Strategy for Reducing Violent Crime (see supra note 22).

25 Deputy Attorney General Lisa O Monaco Gives Keynote Address at ABA's 36th National institute on White Collar Crime, (28 Oct. 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

© Law Business Research 2021

full disclosure of all non-privileged information about individuals and, alternatively, disclosure of individuals 'substantially involved' in wrongdoing. The DOJ will not give discretion to a company or its counsel to determine who meets that threshold of involvement, because the 'department's investigative team is often better situated than company counsel to determine the relevance and culpability of individuals involved in misconduct'.

Individual accountability for wrongdoing 31.1.4

Under US law, criminal prosecution and civil actions may be brought against business organisations including corporations, partnerships, sole proprietorships, government entities and other unincorporated associations, notwithstanding their artificial nature as a legal entity.[26] The prosecution of corporate crime has long been a high priority for the DOJ, with a focus on (1) protecting the integrity of the economic and capital markets by enforcing the rule of law, (2) protecting consumers, investors and business entities against competitors who gain unfair advantage by violating the law, (3) preventing violations of environmental laws and (4) discouraging business practices that would permit or promote unlawful conduct at the expense of the public interest.[27] Under this concept of corporate liability, corporations and other business organisations can be indicted, plead guilty, be convicted of offences, be fined and be required to institute remedial measures to prevent future wrongdoing.[28] Historically, the DOJ's focus on corporate wrongdoing often led to significant settlements with companies, but without any individuals being held accountable for the crimes charged. Following increasing public and judicial criticism about the lack of individual accountability, in September 2015, the DOJ issued a memorandum titled 'Individual Accountability for Corporate Wrongdoing', authored by then-Deputy Attorney General Sally Quillian Yates (commonly referred to as the Yates Memorandum).[29] The Yates Memorandum set forth new policy guidance focusing on prosecuting individuals with responsibility for the crimes for which corporations could be held responsible, and its core principles were incorporated into the US Attorneys' Manual (now the Justice Manual) several months later. In acknowledging the historical challenge of identifying and prosecuting individuals who were aware of or complicit in corporate misconduct, the Yates Memorandum listed six key steps to strengthen the DOJ's pursuit of individual wrongdoers.

26 JM, Principles of Federal Prosecution of Business Organizations, § 9-28.000 et seq., https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

27 Id., at § 9-28.010 (Foundational Principles of Corporate Prosecution).

28 Id., at § 9-28.200 (General Considerations of Corporate Liability).

29 Office of the Deputy Attorney General, DOJ, Individual Accountability for Corporate Wrongdoing (9 Sep. 2015), https://www.justice.gov/dag/file/769036/download. The Yates Memorandum has since been largely incorporated into JM § 9-28.700 (The Value of Cooperation).

© Law Business Research 2021

- *Provision of evidence against individual wrongdoers*: For a company to receive any consideration for co-operation with the government under the Principles of Federal Prosecution of Business Organizations, the company must completely disclose to the DOJ all relevant facts about any individual misconduct. This includes identifying all individuals responsible for the misconduct at issue, regardless of their position, status or seniority at the company.
- *Investigative focus on individual wrongdoers*: Both civil attorneys and criminal prosecutors at the DOJ will now focus on individual wrongdoing from the beginning of any investigation of corporate misconduct.
- *Coordination between civil attorneys and criminal prosecutors*: Civil attorneys and criminal prosecutors at the DOJ will more regularly consult throughout all phases of an investigation of corporate misconduct and will consider bringing parallel civil and criminal proceedings to take advantage of the full range of the government's potential remedies, including fines, imprisonment, forfeitures, restitution, and suspension and debarment.
- *No shielding of individuals from liability*: Absent extraordinary circumstances, no resolution of a case of corporate misconduct will provide protection from criminal or civil liability for individuals. Any release of criminal or civil liability due to extraordinary circumstances must be personally approved in writing by the relevant Assistant Attorney General or United States Attorney.
- *No corporate resolution without individual resolution*: If the investigation of individual misconduct has not concluded by the time authorisation is sought to resolve the case against the corporation, a plan must be implemented by the DOJ prosecutor on how to resolve the matter prior to the end of any statute of limitations period.
- *Increased focus on civil settlements*: Civil attorneys at the DOJ will focus on recovering as much money as possible for the public, regardless of an individual's ability to pay. Instead, the decision as to whether to file a civil action against an individual should focus on the seriousness of the person's misconduct, whether it is actionable, whether the admissible evidence will be sufficient to obtain a judgment and whether pursuing the action reflects an important federal interest.

To some practitioners, the Yates Memorandum merely memorialised the DOJ's existing practice of prosecuting culpable individuals in white-collar cases. However, the requirement that the government prove that defendants intentionally and knowingly violated the law remains a significant hurdle, especially in the context of corporate wrongdoing. Indeed, the Yates Memorandum notes that in cases of misconduct in a large corporate setting 'where responsibility can be diffuse . . . it can be difficult to determine if someone possessed

© Law Business Research 2021

the knowledge and criminal intent necessary to establish their guilt beyond a reasonable doubt'.[30]

In November 2018, the then Deputy Attorney General Rod Rosenstein announced revisions to the Yates Memorandum to restore some of the prosecutorial discretion that had traditionally been afforded to cases involving corporate wrongdoing.[31] Rosenstein's speech, while emphasising that the aggressive targeting of white-collar crime in general and individuals in particular remained a 'top priority', also effectively conceded that the Yates Memorandum's 'all or nothing' approach was somewhat unrealistic. In deviating from a position whereby corporations must identify every individual wrongdoer to obtain co-operation credit, Rosenstein stated that the new policy permits prosecutors to recognise credit when a corporation identifies the individuals who play 'significant roles' in corporate misconduct. The revised policy allowed prosecutors more discretion to agree to credit based on the extent of a corporation's co-operation, while maintaining the position that corporations that failed to co-operate in good faith would remain ineligible for credit.[32] The effective components of the Yates Memorandum, as revised by the Rosenstein comments, were incorporated into the Justice Manual.[33] In March 2019, the DOJ's Corporate Enforcement Policy was revised to incorporate Rosenstein's November 2018 comments to the Yates Memorandum; companies are only required to share information about individuals that are 'substantially involved in or responsible for the misconduct at issue', rather than identifying all individuals responsible for misconduct.[34]

Sentencing 31.2

Generally 31.2.1

Individuals who are convicted of violating a federal criminal law, including white-collar laws, face a range of possible punishments including fines, probation and imprisonment. In determining the nature and range of a potential sentence following a conviction, there are currently two sources of guidance for judges, prosecutors and defence counsel to refer to: criminal statutes in

30 Ibid.

31 Deputy Attorney General Rod J Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

32 Ibid.

33 JM § 9-28.700 (The Value of Cooperation).

34 JM § 9-47.120 (FCPA Corporate Enforcement Policy). The then Assistant Attorney General Brian A Benczkowski echoed Rosenstein's modification to the Yates Memorandum in a speech at the 33rd Annual ABA National Institute on White Collar Crime in March 2019: https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-33rd-annual-aba-national.

© Law Business Research 2021

the United States Code[35] and the United States Sentencing Guidelines (the Guidelines).[36]

In 1984, Congress passed the Sentencing Reform Act (SRA), which led to the creation of the Guidelines.[37] The Guidelines require a score-based analysis focused on a myriad of factors relating to the circumstances of the offence. This analysis leads to one of 43 different offence levels[38] and six criminal history categories.[39] As originally designed, the Guidelines were mandatory. However, in 2006, the US Supreme Court in *United States v. Booker* determined that mandatory application of the Guidelines was unconstitutional and that they are advisory recommendations only.[40] As a result of *Booker*, the Guidelines now act as a starting point for a federal judge to determine what sentence should be imposed, consistent with minimum and maximum sentences set forth in the offence of conviction, as well as the factors set forth in the federal sentencing statute.[41] A review of the Sentencing Guidelines indicates no amendments

35 United States Code [U.S.C.], US Government Publishing Office, https://www.govinfo.gov/app/collection/uscode/.

36 US Sentencing Guidelines Manual (effective 1 November 2018), United States Sentencing Commission, https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf. Because of vacancies on the United States Sentencing Commission, the 2019 Proposed Amendments to the US Sentencing Guidelines lacked the minimum number of affirmative votes to promulgate amendments to the federal sentencing guidelines: https://www.ussc.gov/about/annual-report-2019.

37 18 U.S.C. §§ 3551–586, 3601–742; 28 U.S.C. §§ 991–98. The Sentencing Reform Act of 1984 (SRA) required a federal district court judge to consider each of the factors in the federal sentencing statute, 18 U.S.C. § 3553(a), when crafting a sentence, which included (1) the 'nature and circumstances of the offence' and the defendant's 'history and characteristics', (2) the general purposes of the SRA, (3) the 'kinds of sentences available', (4) the 'pertinent policy statements issued by the U.S. Sentencing Commission', (5) the 'need to avoid unwarranted sentence disparities' between defendants convicted of similar conduct, (6) the 'need to provide restitution to any victims' and (7) the applicable sentence range recommended by the Guidelines.

38 Guidelines § 5A.

39 Guidelines § 4A1.1.

40 543 U.S. 220, 245–46 (2005) (holding that the Guidelines must be considered as an advisory, not a mandatory, calculation of sentence to be consistent with the Sixth Amendment right to a trial by jury). The *Booker* court held that the federal sentencing statute requires judges to consider the Guidelines' sentencing range and to 'impose sentences that reflect the seriousness of the offense, promote respect for the law, provide just punishment, afford adequate deterrence, protect the public, and effectively provide the defendant with needed educational or vocational training and medical care.' Ibid., at 259, 260 (citing 18 U.S.C. § 3553(a)).

41 18 U.S.C. § 3553(a). The federal sentencing statute defines the factors to be considered by the judge in imposing a sentence on a defendant and mandates that it should be 'sufficient, but not greater than necessary'. 18 U.S.C. § 3553(a)(2). As a result of the Supreme Court's ruling in *Booker*, courts should consider the Guidelines as one factor in imposing a sentence, but a judge may impose a different sentence if other § 3553(a) factors suggest that the Guidelines'

© Law Business Research 2021

have been adopted since 2018 and none have been proposed since 2019, likely due to vacancies on the US Sentencing Commission.

Imprisonment 31.2.2

The federal prison system is operated by the Bureau of Prisons and currently contains 156,098 inmates in more than 140 facilities located throughout the United States.[42]

When calculating a potential sentence of imprisonment under the Guidelines, the judge first looks to the 'base offence level' applicable to the defendant's conviction,[43] and adjusts that upward or downward for specific applicable offence characteristics, special instructions and other factors to calculate the 'total offence level'.[44] Next, the judge determines the defendant's criminal history category (categories I to VI), which is increased by prior criminal convictions.[45] Once the total offence level and criminal history category are determined, the judge arrives at the recommended sentence by identifying the applicable range in the Guidelines' sentencing table.[46] Judges have discretion to depart upward or downward from the recommended range upon finding that the case includes one or more aggravating or mitigating circumstance 'of a kind not adequately taken into consideration' by the Guidelines.[47] Judges may also depart from the Guidelines if the government moves for a downward departure based on the defendant's substantial assistance in another case.[48] In any case, the judge must state in writing the specific reasons for imposing a sentence outside the applicable Guidelines sentencing range.[49]

Fines 31.2.3

An individual convicted of a federal crime may also be sentenced to pay a monetary fine.[50] Many criminal statutes set forth the range of fines that may be assessed upon conviction; for those felonies whose statute does not so specify, the fine is set at not more than US$250,000.[51] As with terms of imprisonment,

---

range is inappropriate. See *Kimbrough v. United States*, 552 U.S. 85, 91 (2007) ('A district judge must include the Guidelines range in the array of factors warranting consideration.')

42 Federal Bureau of Prisons Statistics (updated 3 November 2021), https://www.bop.gov/about/statistics/population_statistics.jsp.

43 Guidelines §§ 1B1.1(a)(1), 1B1.2(a).

44 Guidelines §§ 1B1.1(a)(2), 1B1.1(c).

45 Guidelines § 1B1.1(a)(6).

46 Guidelines § 1B1.1(a)(7).

47 Guidelines § 5K2.0 (quoting 18 U.S.C. § 3553(b)).

48 Guidelines § 5K1.1. See also *United States v. Gall*, 552 U.S. 38, in which the US Supreme Court held that federal appeals courts may not presume that a sentence is unreasonable if it falls outside the range recommended by the Guidelines.

49 18 U.S.C. § 3553(c)(2).

50 18 U.S.C. § 3571(a).

51 18 U.S.C. § 3571(b)(3).

© Law Business Research 2021

the Guidelines contain a fine table that provides the court with an advisory minimum and maximum fine range for defendants, based on the offence level at which the defendant is sentenced.[52]

Judges may depart upwards or downwards from the Guidelines' fine range based on factors such as a defendant's ability to pay, any restitution the defendant must make, the potential for collateral consequences the defendant may face (such as civil litigation) and other equitable considerations.[53]

31.2.4 Probation

The US Probation and Pretrial Services System supervises individuals sentenced to a term of probation to ensure compliance with conditions imposed by the sentencing judge. Probation is a sentence in and of itself, and may be used as an alternative to imprisonment.[54] When imposing probation, the sentencing judge must consider the Guidelines[55] as well as the factors set forth in the SRA.[56]

The Guidelines contain a list of standard conditions that are recommended in all cases of probation,[57] along with a list of special conditions to be considered under certain circumstances.[58] A judge may impose additional conditions on a defendant's probation term that are reasonably related to the nature and circumstances of the offence, the history and characteristics of the defendant, and the goals of sentencing.[59] In all cases, the court must provide the defendant with written notice of the conditions.[60] The court may revoke a defendant's probation at any time before the end of its term for any violation of a probation condition that occurs during that time.[61] Supervised release is another form of post-incarceration supervision, where a probation officer monitors the defendant and ensures compliance with conditions for release. Although

52 Guidelines § 5E1.2. For example, if a defendant is convicted of bank fraud and is sentenced at offence level 18, the fine table sets a guideline range of US$6,000 to US$60,000. Ibid.

53 Guidelines § 5E1.2(d).

54 18 U.S.C. § 3561; Guidelines § 5B1.1.

55 See, e.g., *United States v. Toohey*, 448 F.3d 542, 546-47 (2d Cir. 2006) (holding that a departure from the Guidelines' prison recommendation to probation may be warranted, but the district court should nonetheless 'consider the Guidelines and all of the other factors listed in § 3553(a)').

56 The SRA directs the sentencing judge, when imposing probation, to consider several factors, including (1) the nature of the offence and history and characteristics of the defendants, (2) the need for just punishment, deterrence, or public protection, (3) the need to provide the defendant with educational or vocational training, medical care, or other correctional treatment, (4) the types of sentences available, (5) the Guidelines, (6) the need to avoid unwarranted sentencing disparities between defendants with similar records for similar conduct, and (7) the need to provide restitution to victims. See 18 U.S.C. § 3553(a).

57 Guidelines § 5B1.3(c).

58 Guidelines §§ 5B1.3(d), (e).

59 Guidelines § 5B1.3(b).

60 18 U.S.C. § 3563(d).

61 18 U.S.C. § 3564(e), 3565(a).

© Law Business Research 2021

similar to probation, a term of supervised release is a period of supervision that follows the full period of incarceration, whereas probation is a substitute for imprisonment.

Confiscation of assets 31.2.5

Pretrial asset freeze orders 31.2.5.1

Under US law, the government can seek a temporary order freezing an individual's assets, in both the civil and criminal contexts, before a case is proven at trial. In civil enforcement matters, regulators can seek asset freezes from an administrative law judge once an action is initiated, often in *ex parte* proceedings at which the respondent is not present. In criminal matters, prosecutors can seek asset freeze orders from a district court based on a showing of probable cause that the assets are subject to permanent forfeiture.

The Supreme Court in *Luis v. United States* held that the pretrial restraint of a criminal defendant's assets – which assets were not 'tainted' by the alleged criminal conduct – violates the Sixth Amendment right to counsel.[62] As a result, while the government can freeze and seize assets pretrial that are believed to derive from criminal activity, its ability do so for 'untainted' assets are trumped by the defendant's Sixth Amendment right to counsel of choice.

Civil and criminal asset forfeitures 31.2.5.2

Permanent government confiscation of property is called a 'forfeiture'. There are generally three types of forfeiture proceedings available to US law enforcement and prosecutors: administrative, civil and criminal.[63]

Administrative forfeiture permits a federal agency to seize personal (non-real) property without initiating a judicial proceeding. The authority derives from the Tariff Act of 1930, which states that the following types of property are eligible for administrative forfeiture: (1) property whose value does not exceed US$500,000; (2) merchandise whose importation is prohibited; (3) a conveyance used to import, transport or store a controlled substance; and (4) a monetary instrument.[64]

Civil forfeiture is an *in rem* proceeding that is brought directly against a piece of real or personal property that is involved, derived from or traceable to one or more enumerated federal crimes.[65] The property itself is the defendant and no charge against an individual is necessary. In a civil forfeiture proceeding, the government must prove, by a preponderance of the evidence, that the property

62 136 S. Ct. 1083 (2016).

63 The DOJ's Asset Forfeiture and Money Laundering Section publishes an Asset Forfeiture Policy Manual, most recently updated in 2019, to set forth DOJ policy and provide guidance to US Attorneys' Offices on the DOJ's Asset Forfeiture Program. See Asset Forfeiture Policy Manual, available at https://www.justice.gov/criminal-afmls/file/839521/download.

64 19 U.S.C. § 1607.

65 18 U.S.C. §§ 981 and 983-5.

© Law Business Research 2021

is subject to forfeiture.[66] If a claimant raises an innocent owner defence, he or she has the burden of proving that the claimant is an innocent owner of the property by a preponderance of evidence.[67]

Criminal forfeiture is an action brought as part of a criminal case against a defendant, not against a specific asset. It is an *in personam* action and requires the government to include a forfeiture charge against the defendant in the indictment, and prove that the property was used or derived from one or more enumerated federal crimes.[68] The indictment or criminal information must contain notice to the defendant that the government is seeking forfeiture of property as part of any sentence.[69] If a defendant disposes of the original asset subject to forfeiture, the government may obtain substitute assets[70] or may obtain a money judgment in an amount equal to the criminal proceeds.

A defendant can challenge the dollar amount of a criminal or civil forfeiture as a violation of the Eighth Amendment to the US Constitution, which restricts the government's ability to impose 'excessive fines' as punishment.[71]

31.2.6 Compensation orders

Under the Mandatory Victims Restitution Act of 1996,[72] defendants convicted of certain federal crimes, as well as defendants sentenced to probation, must in most circumstances make restitution to each of their victims in the full amount of the victim's financial losses that resulted from the defendant's crimes.[73] Restitution by the defendant must be ordered regardless of the

66 18 U.S.C. § 982(c)(91).

67 18 U.S.C. § 982(d)(1).

68 18 U.S.C. § 982.

69 Fed. R. Crim. P. 32.2(a).

70 Prosecutors may seek the forfeiture of 'substitute assets' in place of tainted property when certain conditions are met. See 21 U.S.C. § 853(p) (incorporated by reference in various criminal forfeiture statutes).

71 See *Alexander v. United States*, 509 U.S. 544, 558–59 (1993) (holding that the excessive fines clause of the Eighth Amendment applies to *in personam* criminal forfeiture for purposes of determining whether a penalty is 'excessive'); *Austin v. United States*, 509 U.S. 602, 609, 610 (1993) (holding that the excessive fines clause applies to civil forfeitures of conveyances and real property used to facilitate the transport, sale, or possession of controlled substances under 21 U.S.C. § 881(a)(4) and (7)).

72 Pub. L. No. 104–132, § 204, 110 Stat. 1214, 1227 (codified at 18 U.S.C. §§ 3556, 3663 and 3664).

73 See *Hughey v. United States*, 495 U.S. 411, 413 (1990) (holding that restitution may only be awarded for losses resulting from the specific conduct for which the defendant was convicted). The *Hughey* decision was subsequently modified by Congress pursuant to the Crime Control Act of 1990, which authorised courts to order any restitution amount agreed to in a plea agreement, and broadened restitution payable to any person directly harmed by the defendant's conduct in the course of a scheme or conspiracy. See Pub. L. No. 101-647 § 2509, codified at 18 U.S.C. § 3663. See also *Lagos v. United States*, 138 S. Ct. 1684 (2018) (limiting the ability of corporate victims to obtain restitution orders for legal fees and other costs incurred in conducting internal investigations into a defendant's misconduct).

© Law Business Research 2021

defendant's economic circumstances, or any third-party compensation received by the victim.[74]

Collateral consequences of conviction 31.2.7

In addition to imprisonment, fines, probation, forfeitures and other direct sanctions that may be imposed by a criminal court, there are a number of other federal, state and local legal and regulatory restrictions that may result as 'collateral consequences' of a criminal conviction.[75] They are imposed automatically upon conviction, even if not expressly included in the criminal court's judgment, or by action of a civil court or administrative agency.

74 18 U.S.C. § 3664(f)(1)(A)-(B). Judges must, however, consider a defendant's economic circumstances when deciding on a payment schedule and form of restitution. 18 U.S.C. § 3664(f)(2).

75 See ABA Standards for Criminal Justice, Collateral Sanctions and Discretionary Disqualification of Convicted Persons, Standards 19-2.1 and 19-3.1 (3d ed. 2003), https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/crimjust_standards_collateral_blk/#2.1.

© Law Business Research 2021

32

Extradition

Ben Brandon and Aaron Watkins[1]

32.1 Introduction

Extradition is the legal process by which one state formally requests from another, usually on the basis of a treaty or equivalent legal arrangement, the surrender of a person accused or convicted[2] in the 'requesting state' of the commission of a criminal offence within its jurisdiction.[3] It is a manifestation of the international obligation on states either to surrender a criminal for prosecution abroad or prosecute him or her before their own courts (*aut dedere aut judicare*).

The process in a state that receives an extradition request of deciding whether to surrender a requested person is not a 'trial' of the allegation in the requesting state, nor a review of any conviction imposed. The requested state is not evaluating evidence to assess innocence or guilt. Broadly speaking, the decision is based on an assessment of whether the formal requirements to

1 Ben Brandon is a barrister and a partner at Mishcon de Reya LLP and Aaron Watkins is a barrister at Cloth Fair Chambers.

2 Extradition may not be used for the purposes of investigation, conducting interviews or generally gathering evidence; there are well established methods of mutual legal assistance for these activities.

3 Although similarly concerned with 'expulsion' and therefore not infrequently confused with deportation, extradition is an entirely distinct legal concept. Whereas deportation generally concerns the removal of individuals to foreign states in which they have residency rights from a country where they do not, and is often entirely unconnected to criminality, extradition depends on a request for the return of an individual for alleged criminal conduct.

© Law Business Research 2021

accede to the extradition request are present and whether any of a number of prescribed 'defences' to extradition should bar surrender.[4]

Bases for extradition 32.2

The main mechanisms by which states enter extradition relationships are: (1) bilateral treaties, (2) multilateral treaties or conventions, and (3) *ad hoc* special arrangements.[5]

States have been engaged in formal extradition by way of bilateral treaty since at least 1284 BC.[6] In more modern times, bilateral treaties have remained an important legal basis by which states form extradition relationships: for example, the current arrangements between the United States and the United Kingdom are established in the UK–US extradition treaty of 2003.[7]

In recent decades, however, multilateral treaties and conventions have become similarly important. The most prominent example is perhaps the European arrest warrant scheme, which came into force on 1 January 2004 in EU Member States by way of a European Framework Decision on Extradition.[8] An EU-wide measure was considered desirable for a number of reasons, including to ensure that the initiative of open borders and free movement within the European Union did not also make evading justice easier. It was introduced to facilitate a speedier, simplified process of surrender between Member States that did not require requesting states to produce any evidence to support their requests for extradition (instead relying on the provision of 'information'). At the heart of the simplified, expedited process was mutual trust and co-operation grounded on an assumption of broadly aligned systems and standards across Member States.

Other notable multilateral arrangements include the European Convention on Extradition 1957, which despite its title is the arrangement that governs (*inter alia*) the United Kingdom's extradition relationship with South Africa, and is an instrument which Israel and the Republic of Korea have also ratified. Large multilateral arrangements have also been implemented elsewhere in the world, for example the Inter-American Convention on Extradition between

4 Under some extradition schemes, a court may (where it is required by the relevant extradition law) consider whether the requesting state has provided sufficient evidence of a 'case to answer', also referred to as a *prima facie* case. Generally, this is a decreasingly common requirement in extradition proceedings, as the growing trend is to assess the sufficiency of 'information', rather than to require 'evidence' of a case to answer.

5 Not considered further in this chapter, these are usually diplomatically negotiated one-off measures in relation to particular cases of interest to the requesting state.

6 A treaty between Egyptian Pharaoh Rameses II and Hittite ruler Hattusilis III.

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243246/7146.pdf.

8 https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF.

© Law Business Research 2021

16 states in South America, Central America and the Caribbean.[9] In the Middle East, the Riyadh Arab Agreement for Judicial Co-operation constitutes a similar multilateral arrangement.[10]

32.3 Core concepts

Whether the foundation for extradition is a bilateral or multilateral instrument, certain core concepts enable extradition, or operate to prevent it.

32.3.1 Double (dual) criminality

Under virtually all formal extradition arrangements an offence will not be 'extraditable' or an 'extradition offence' unless the conduct alleged constitutes, and would have done so at the relevant time, an offence under the laws of the requested state.[11] In other words, where a requested state concludes that the alleged conduct would not be criminal under its own domestic laws, it is not entitled to extradite.

The focus of this test is much more commonly considered to be the nature of the conduct alleged rather than a comparison of the juridical elements of the offences.[12] As long ago as 1878 the reason for this was recognised as follows: '[T]he . . . magistrate cannot be expected to know or interpret the foreign law. It is not desirable that he should be required to do more than to see that the facts proved constitute *prima facie* an offence which would have been within judicial cognizance if done in this country.'[13]

The 'conduct test' requires the transposition of the alleged conduct to the requested state to assess whether it would be criminal there. The depth at which this transposition of facts needs to occur is a matter of some debate, particularly in respect of certain types of crime. For example, fiscal offences, which are often highly state-specific are unlikely to satisfy a transposition exercise that 'exports' the specifics of the tax regime to the requested state. For this reason, tax offences often receive exemptions from the rigours of a double criminality transposition exercise.[14] A further significant departure from the general requirement of double criminality is the use of lists of certain types or categories of criminal

9 In force in March 1992.

10 Part VI. In force in October 1985. The following governments are signatories to this agreement: Jordan, United Arab Emirates, Bahrain, Tunisia, Algeria, Djibouti, Saudi Arabia, Sudan, Syria, Somalia, Iraq, Oman, Palestine, Qatar, Kuwait, Lebanon, Libya, Morocco, Mauritania and Yemen.

11 Other requirements are sometimes added to strengthen this requirement, for example requiring the conduct to be capable of punishment in excess of a specified minimum to ensure a baseline of seriousness.

12 See, for example: *Norris v. Government of the United States* [2008] 1 A.C. 920.

13 Report of the Royal Commission on Extradition (1878).

14 See, for example, Second Additional Protocol to the European Convention on Extradition 1957, Chapter II, Article 2, and Council Framework Decision 2002/584/JHA on the European arrest warrant, Article 4(1).

© Law Business Research 2021

offending, which, if relied upon by the requesting state automatically bypass the need for a double criminality assessment in the requesting state.[15]

Specialty 32.3.2

A further, and near universally acknowledged, core principle of extradition is specialty.[16] The principle demands that when a requested person has been extradited, they can only be prosecuted in relation to an offence for which the extradition was ordered. Prosecution or detention in connection with additional offences is usually only permitted where the extradited person is first afforded a period to leave the state to which he or she was surrendered, or where consent has been sought from (and provided by) the requested state.

'Political motivation' 32.3.3

Originally, the focus of the interplay between politics and extradition was the 'political offence' exception to extradition: in summary, the prohibition of extradition for offences committed for a political reason. The origins of this concept are in asylum and relate to the practice of providing refuge to those whose conduct was considered to be politically driven. As Lord Diplock famously observed, a degree of neutrality was needed in the approach to conflicts between regimes and their potential successors because '[t]oday's Garibaldi may well form tomorrow's government'.[17] However, a widely acknowledged lack of clarity about the scope of what constituted a 'political offence', in particular in the context of the treatment of terrorists in the second half of the 20th century, led to a shift in how extradition arrangements sought to protect requested persons from persecution.

That shift has been to import the approach and concepts found in the 1951 Refugee Convention to create 'non-discrimination' protections in extradition, which prevent extradition where it can be shown that an extradition request has been issued to prosecute a requested person on account of their 'race, religion, nationality, gender, sexual orientation or political opinions'[18] or, where it can be established that a requested person might be prejudiced at trial or detained by reason of the same considerations.[19] The scope of what consti-

15 See, for example, Council Framework Decision 2002/584/JHA on the European arrest warrant, Article 2(2).

16 Sometimes referred to as 'speciality' to achieve linguistic equivalence with the French word '*spécialité*' and German '*spezialität*'.

17 *Cheng v. Governor of Pentonville Prison* [1973] AC 931.

18 Also referred to as the 'extraneous considerations' bar to extradition.

19 See, for example, UK Extradition Act 2003, ss.13 and 81.

© Law Business Research 2021

tutes 'political opinions' has been a source of some uncertainty, but the better view remains that the concept should receive a wide interpretation.[20]

32.3.4 Double jeopardy (ne bis in idem)

Most extradition arrangements also recognise as a bar to surrender the *ne bis in idem* principle, which prevents a requested person from being surrendered where it would result in his or her prosecution twice for the same offence in different jurisdictions. The ability to rely on the double jeopardy bar does not necessarily require the offence or conduct that is the subject of the extradition proceedings to map identically onto the previous conviction or acquittal relied on. It should be available as a protection where the requesting state seeks to prosecute in respect of facts so closely related that it would be unfair for a second prosecution to take place.[21]

32.3.5 Human rights

Fundamental human rights concepts and standards have become increasingly relevant to extradition, particularly for Contracting States to the European Convention on Human Rights (ECHR). There are two central aspects to human rights protections in the extradition context: the court which applies these human rights standards must not act inconsistently with them, and further, extradition must be barred where surrender would be incompatible with rights conferred by the ECHR, even where the requesting state is not itself a Contracting State.

In practice, the ECHR articles most frequently relied on in extradition cases are Article 3 (the prohibition of torture and inhuman treatment), Article 6 (the right to a fair trial) and Article 8 (the right to a private and family life). Each of these commonly invoked provisions has a well-established body of case law at both national and supranational court level.

Article 3 ECHR is frequently deployed in connection with conditions of detention in the requesting state. The demonstration of serious systemic failings within a prison estate, or the existence of specific characteristics rendering an individual particularly vulnerable in detention can give rise to the necessary 'substantial grounds' for believing there is a 'real risk' of a breach of this protection. It is an increasingly common response of requesting states faced with such arguments to provide detailed, specific diplomatic assurances to the requested state to meet any potential Article 3 risk.

---

20 *Emilia Gomez v. SSHD* [2000] INLR 549: It is not necessary to demonstrate the only motive behind a request or prosecution is political, it is sufficient for political reasons to part of the motivation. It is not necessary to show political action or activity. Political opinions can be those imputed to the requested person. It is also unhelpful to create rigid distinctions between narrowly political opinions and other opinions of political relevance, such as economic opinions.

21 See, for example, *Fofana v. Deputy Prosecutor Thubin Tribunal de Grande Instance de Meaux France* [2006] EWHC 744 (Admin).

© Law Business Research 2021

Article 6 ECHR as a bar to extradition most frequently arises in conjunction with the political motivation or extraneous consideration bar, where a requested person seeks to argue that the origins and purpose of the request for the extradition would expose him or her to an unfair trial process if surrendered. In doing so, the particular context of extradition requires not merely the demonstration of a risk of a violation of fair trial principles, but the real risk of a *flagrant* denial of justice.[22]

Article 8 ECHR does not confer absolute rights. While extradition will inevitably infringe requested persons' and their families' rights, reliance on Article 8 to prevent extradition will depend on the court balancing competing interests and considering the proportionality of the interference caused by extradition, and its justification. In doing so, unsurprisingly courts consistently recognise the intrinsic and powerful interests in giving effect to extradition arrangements and in ensuring those charged with crimes face trial. Added to that, courts will frequently weigh factors such as the seriousness and age of alleged conduct on the one hand, and the impact of extradition on children and vulnerable dependents on the other. Overall, it is only in comparatively rare cases that the Article 8 rights of a requested person outweigh the interests in surrender.

Trends in extradition 32.4

Growth of international co-operation in criminal justice 32.4.1

Population growth and global migration has provided the major impetus for the increased use of extradition in the past twenty years. A key criminal justice response to the free movement of peoples introduced following the entry into force of the Treaty of Maastricht[23] was the Framework Decision which provided for the mutual recognition of warrants of arrest issued by judicial authorities across the European Union.[24] Non-EU states have dusted off rarely used extradition treaties that have been in existence since the late nineteenth century, and a profusion of new extradition treaties that permit extradition between states that formerly had no extradition arrangements at all have been created. In 2020, Kuwait and Morocco were designated under Part 2 of the Extradition Act 2003 and added to the ever-lengthening list of states that the United Kingdom now regards as 'extradition partners'.[25]

The importance of the text of the international convention creating the extradition relationship depends on whether the state directly implements treaty provisions into its domestic law (monist states) or whether local law

22 *Othman v. United Kingdom* [2012] ECHR 56 at paras. 258–60.

23 https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf.

24 Council Framework Decision 2002/584/JHA of 13 June 2002.

25 The Extradition Act 2003 (Amendments to Designations) Order 2020. Statutory Instrument No. 265 of 2020.

© Law Business Research 2021

is required to give effect to treaty obligations (dualist states). In the United Kingdom, and generally across all common law jurisdictions, domestic implementing legislation is required, and the text of the treaty is of secondary importance. In many civil law jurisdictions, the provisions of the treaty or other international arrangement such as the Framework Decision have direct effect in local law.

One of the more controversial features of the European arrest warrant scheme introduced by the Framework Decision was that all Member States agreed that the Court of Justice of the European Union (CJEU) would have the final say in interpreting relevant provisions of the Framework Decision, and that its findings would bind local courts in Member States. For many in the Brexit campaign who opposed the EAW, this feature of the Framework Decision represented a surrender of UK sovereignty to the CJEU.

32.4.2 The 'judicialisation' of the extradition process

The increased importance of judicial as opposed to political decision-making in extradition cases is part of a growing trend across all extradition arrangements, both within and outside the European Union, between EU and non-EU states, and states wholly outside the European Union. In the past, extradition treaties were often based on simple lists of offences for which extradition would be ordered. The requesting state would have to provide evidence in support of the request, which was only received and admitted by the executing court if it satisfied a complex and arcane set of rules. Extradition was often only barred for political or military offences or by reason of the passage of time, and human rights challenges were unheard of. Although courts were involved in assessing evidence and applying the relevant provisions of the applicable treaty or domestic law, the decision as to whether to proceed with the extradition request in the first instance, and ultimately whether to order extradition at the conclusion of the hearing was almost always taken by the executive.

In many states, the decision to extradite still remains a decision taken by the executive, but the courts of the executing state have a much greater role than historically has been the case. In EU states and the United Kingdom, the decision to extradite is now almost always made by a court rather than the executive. As the ECHR and the jurisprudence of the European Court of Human Rights has become more embedded in the domestic legal orders of EU states, responsibility for making what were regarded as political decisions of a legal character was removed from the executive, and became the exclusive preserve of the courts.

Decisions as to whether to extradite a requested person are now made upon the basis of an established and well-defined set of rules, in an open and public forum, by tribunals whose decisions can be challenged in superior courts. In this way, not only have the numbers of extradition cases increased exponentially in recent years, but also their visibility and accessibility. Where the executive does retain a role in the process, as in the United Kingdom, where the Secretary of State for the Home Department makes the decision to order a person's

© Law Business Research 2021

extradition where the request is received from a state outside the European Union, that decision is ordinarily heavily circumscribed. There is little or no room for the government to take a different decision from the courts, and when it has done so, further reductions in the scope of executive decision-making has followed.[26]

Courts are also required to make a far greater number of individual decisions in extradition cases. As above, most states now use the 'conduct test' rather than a simple list-based system to determine whether an extradition crime is made out. This means that a far greater number of offences are potential extradition crimes and the court is required to examine the underlying conduct alleged in each request. Many states have human rights and other bars based on anti-discrimination clauses in their local laws requiring careful judicial consideration. In complex frauds that may have a political dimension, the executing court is often required to examine a large volume of documentary material and consider the reports of expert witnesses in deciding whether there is *prima facie* evidence of an extradition crime and whether the requested person is able to make good a challenge to the request on human rights or other grounds.

Once executive authority to proceed with a request had been given, traditionally the extradition court in the executing state would have considered whether the requesting state had adduced sufficient evidence in receivable and admissible form to demonstrate that the requested person had a case to answer. Many modern extradition arrangements have not only done away with the requirement for documents to be bound and sealed, but have also dispensed with the requirement to prove a *prima facie* case on the request.

Decreasing requirement to provide evidence of a prima facie case 32.4.3

The clearest example of this development is the European arrest warrant, which requires either a box to be ticked indicating a Framework List offence is the subject of the request, together with a short description, usually no more than a paragraph, of the conduct alleged against the requested person. In the United Kingdom, there are other 'trusted extradition partners' such as the 'Five Eyes' states and other Member States of the Council of Europe who likewise, are not required to provide evidence of a *prima facie* case in the extradition request.[27] All that is required is an affidavit, usually from a state prosecutor,

26 The Crime and Courts Act 2013 was enacted following then-Secretary of State Theresa May's decision to block the extradition of computer hacker Gary McKinnon to the United States. The Act introduced the 'forum bar', at Extradition Act, section 83A, which provides that the extradition of a person is barred by reason of forum if the extradition would not be in the interests of justice.

27 'Five Eyes' is an alliance between the intelligence agencies in Australia, Canada, New Zealand, the United Kingdom and the United States. Council of Europe states that are not within the European Union are Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Liechtenstein, Monaco, Montenegro, North Macedonia, Norway, Republic of Moldova, Russian Federation, San Marino, Serbia, Switzerland, Turkey and Ukraine.

© Law Business Research 2021

setting out information on which a judge at the extradition hearing can determine whether an extradition crime is made out. Such affidavits often do no more than recite the conduct imputed to the requested person in the domestic indictment or the factual basis of that person's criminal conviction together with the key procedural milestones in the domestic criminal case, the current whereabouts of the person sought, some personal information about them and details of the relevant local law, charges, indictment or conviction.

32.4.4 Expedition in the process

Whether or not the courts in the executing state require the requesting state to provide evidence of a *prima facie* case, most modern extradition arrangements are designed to promote expedition. Swift decision-making is not only a foundational objective of the Framework Decision but is given effect by the simplified procedure of mutual recognition of judicial decisions. Time limits imposed by domestic law also attach to the various procedural stages of an extradition hearing. In the United Kingdom, these time limits are found in the Extradition Act 2003, the Criminal Procedure Rules and several relevant practice directions.[28] The most prominent example of this was the strictly enforced time frame for serving and filing notices of appeal from the decision of the judge at the extradition hearing. Until recently there were no circumstances in which time could be extended to permit late service of an application for permission to appeal, which is seven days in the case of Part 1 Extradition Act 2003 cases and 14 days for all other requests.[29] However, the obvious potential for injustice caused by such inflexible adherence to the principle of expedition was tempered by enabling an extension of time where a requested person 'did everything reasonably possible to ensure that the notice was given as soon as it could be given'.[30]

Notwithstanding the increased role of the courts, the multiplicity of issues that are raised in extradition hearings and the opportunities for review and appeal, extradition requests from states that are outside the European Union are also moving through the courts increasingly swiftly. In part, this is because as the number of cases increases, issues are litigated with greater frequency, which results in greater clarity in decision-making and fewer legal and procedural uncertainties. As specialised courts, judges and legal professionals acquire an intimate knowledge of this niche practice area, greater efficiencies are introduced into the process and more cases are dealt with year on year.

28 Criminal Procedure Rules 2015 (the Criminal Procedure Rules 2020 come into force on 5 October 2020) and Practice Directions.

29 Extradition Act 2003, ss.26(4), 28(5), 105(5) and 108(4)

30 ibid., ss.26(5), 103(10), 108(7A)

© Law Business Research 2021

Contemporary issues in extradition 32.5

US extraditions and the forum provisions in UK law 32.5.1

A major issue that has been the cause of tension and controversy in recent years, particularly in the United Kingdom, is the extraterritorial reach of United States' law enforcement and its impact on the nature and frequency of extradition requests received. It has proved marginally less controversial in many other European states that tend not to extradite their own nationals. France, Belgium, and Germany are obvious examples of states that will not extradite their citizens to the United States, regardless of the seriousness of the offences disclosed by the request. This constitutional protection against extradition arises from how such states exercise criminal jurisdiction, which is in accordance with the nationality principle. Hence a crime committed abroad by a French citizen is triable in a French court, wherever in the world the conduct occurred. In common law states, criminal jurisdiction is usually exercised in accordance with the territorial principle. In the United Kingdom, crimes committed abroad are generally not justiciable in domestic courts, which have jurisdiction to try crimes committed within UK territory. A UK citizen who commits a crime abroad can only be tried in the courts located in the territory of the state where the conduct occurred, unless the crime was of a certain character.[31]

The United States has traditionally exercised its jurisdiction territorially, but in recent years has increased the number of offences over which it claims extraterritorial jurisdiction. As a general rule of thumb, any offence which is committed outside the territory of the United States that uses the banking system in the United States or which is regarded as targeting US interests or citizens is potentially justiciable in a US criminal court. The evolution of the extraterritorial reach of US law enforcement is not purely legal in origin. Allied to the expansion of a jurisdiction that was traditionally exercised territorially is an appetite among US prosecutors, particularly in the Southern District of New York and the Departments of Justice and Homeland Security, to pursue such cases together with the resources to carry them to a conclusion.

See Chapter 28 on extraterritoriality

An immediate consequence of what is termed in some quarters as the exercise of 'exorbitant jurisdiction' is the high number of extradition requests received from the United States. In response to a freedom of information request made in January 2020, the Home Office in the United Kingdom provided figures confirming that it extradites over twice as many people to the

31 There are exceptions to this general rule, and the United Kingdom has extraterritorial jurisdiction over certain offences, including murder and manslaughter in most circumstances, certain sexual offences against minors, terrorist offences, bribery offences and other crimes attracting species of universal jurisdiction, such as genocide and certain war crimes, and crimes against ships and aircraft, including piracy. In June 2012, the United Kingdom signed the Istanbul Convention which, once ratified, will allow the United Kingdom to prosecute certain other types of criminal conduct committed outside of the United Kingdom, including sexual offences where the victim is aged over 18.

© Law Business Research 2021

United States as the United States extradites to the United Kingdom. Between 1 January 2014 and 31 December 2019, the United States extradited 15 people to the United Kingdom and, in the same period, the United Kingdom extradited 36 people the other way. In 2019 the number extradited from the United Kingdom to the United States (12) was four times the number the United States sent to the United Kingdom. Between 2014 and 2020, both countries were more likely to extradite a UK national than a US national; the United Kingdom extradited 11 of its nationals (30 per cent) and eight US nationals (22 per cent) to the United States, while the United States extradited five UK nationals (33 per cent) and four of its nationals (26 per cent).[32]

A number of high-profile cases in which the United States has sought the extradition of UK nationals whose conduct was mainly or exclusively committed in the United Kingdom have proved particularly controversial in recent years and has led to a change in the UK law by the introduction of the 'forum test' in the revised section 83A of the Extradition Act 2003.[33]

The underlying aim of the forum provisions is to prevent extradition where the offences can be fairly and effectively tried in the United Kingdom, and it is not in the interests of justice that the requested person should be extradited. The matters relevant to an evaluation of 'the interests of justice' for these purposes are found in section 83A(2)(b). The forum provisions do not leave to the court the task of some vague or broader evaluation of what is just. Nor is the bar a general provision requiring the court to form a view directly on which is the more suitable forum to try a particular case.[34]

Although it is in US extraditions that forum challenges tend to attract public attention (and at the time of writing there are a number of high-profile US cases focusing on the forum bar pending consideration by the High Court), forum-based challenges are now available to requested persons in all extradition requests executed by a UK court, wherever they originate. To date the forum provisions have not led to a significant reduction of extraditions of UK citizens to the United States, but have undoubtedly caused extradition practitioners to consider raising challenges to the exercise of extraterritorial jurisdiction by all states, not just the United States.

32.5.2 Extradition and Interpol red notices

Interpol is an organisation that collects and disseminates information to the global law enforcement community. Where it receives that information from and what is done with it has come under increasing scrutiny in recent years,

32 Letter from the Home Office to Ben Brandon, Mishcon de Reya LLP, dated 6 April 2020. FOI Reference: 57368.

33 The 'forum bar' in the Extradition Act 2003, s.83A, was inserted by the Crime and Courts Act 2013, s.50 and Schedule 20, para. 6.

34 *Love v. United States* [2018] EWHC 172 (Admin) and *Scott v. United States* [2018] EWHC 2021 (Admin)

© Law Business Research 2021

from outside the organisation, and within it.[35] The use of red notices is of ever increasing relevance to extradition practitioners, as their use (and abuse) is often closely linked to the making of a formal request for extradition.

In general, an Interpol national control bureau (NCB) in the territory of the requesting state will receive notification from a local police department, prosecutor or court that a person is wanted and domestic searches have not located the individual concerned. If a decision has been made to prosecute that person, the NCB will usually request that Interpol HQ in Lyon, France, issue a red notice requesting that the person be located, arrested and detained pending receipt of an extradition request. The red notice is generally circulated among NCBs in all Interpol Member States.[36] It is acted on in different ways, depending on the constitutional arrangements of the state in which the person sought is located.

Broadly speaking, dualist states tend not to arrest and detain on red notices, whereas monist states do. Most civil law jurisdictions will arrest and detain on a red notice pending receipt of a formal request for extradition for a prescribed period, often around 40 days. Common law states traditionally did not arrest and detain on red notices, instead requiring receipt of a formal request for extradition before a domestic arrest warrant is issued by a court.

That position will change when the Extradition (Provisional Arrest) Act 2020 comes into force.[37] This legislation is designed to permit the rapid arrest of persons sought by law enforcement in so-called 'trusted states' in Category 2 territories without having to wait for the arrival of a formal request for extradition so as to fill what has been described as a 'capability gap', where those accused or convicted of serious crimes in non-EU states cannot be arrested immediately when found in the United Kingdom. Where such trusted states request Interpol to circulate a red notice for a requested person, the Act will give UK police the power to arrest and detain on such notices provided that a certificate has been issued by the National Crime Agency (NCA).

Among other things, the NCA must certify that the red notice or 'request for the person's arrest' is 'valid' and is for a 'serious extradition offence' and that issue of the certificate would be 'appropriate' to the seriousness of the conduct constituting the offence. A request is valid if it is made in the 'approved way' and contains a statement that the requested person is sought for the purpose of prosecution or to serve a sentence of imprisonment. In accusation cases, the

35 The TRAP Act, introduced by US Congress in 2019, recommended that the United States should use its influence at Interpol to enhance the screening of requests for notices, to prevent abuse and to encourage penalisation or suspension of countries from Interpol that persist in making improper or politically tainted requests for deletion and extradition. In an attempt to increase transparency, the Commission for the Control of Interpol's Files has, in recent years, published a number of redacted decisions on compatibility with the Interpol Constitution and Rules.

36 Interpol has 194 Member States. Currently the only recognised country that is not a member is North Korea.

37 https://www.legislation.gov.uk/ukpga/2020/18/enacted/data.pdf.

© Law Business Research 2021

NCA must also certify that there is sufficient information about the identity of the offender, the conduct alleged against him or her, the relevant provision in local law said to constitute the offence and the available sentence. In conviction cases, the request must contain particulars of the person's identity, their conviction, and the sentence that may be or has been imposed. A request is made in the approved way if it received by an authority in the Category 2 territory that the NCA 'believes' has the function of making such requests.

The list of 'trusted states' in Schedule A1 to the Act currently includes the other 'Five Eyes' states (the United States, Canada, Australia, New Zealand) plus Liechtenstein and Switzerland.

32.5.3 Extradition and Brexit

For all its critics, the EAW scheme is broadly recognised as providing law enforcement with a swift, proportionate and effective means of securing extradition between EU Member States while providing requested persons with procedural and substantive human rights protections. On 1 January 2021, the Brexit transition period came to an end and the United Kingdom is no longer subject to the jurisdiction of the CJEU. Accordingly, the United Kingdom is no longer entitled to be a party to the Framework Decision and has come out of the EAW scheme.

In its place, on 24 December 2020, the United Kingdom and the European Union agreed the terms of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part (the TCA). The TCA included, at Title VII of Part 3, provisions relating to the surrender of citizens between the United Kingdom and the European Union.

The surrender arrangements contained in the TCA are very similar to those provided for by the Framework Decision and those in place between Norway and Iceland and the European Union. As a result, the United Kingdom's future extradition relationship with EU member states will largely operate as previously. There are, however, a small number of provisions that represent a departure from the EAW scheme.

The TCA provides that the new arrangements are subject to the principle of proportionality, and must take into account:

> *the rights of the requested person and the interests of the victims, and having regard to the seriousness of the act, the likely penalty that would be imposed and the possibility of a State taking measures less coercive than the surrender of the requested person particularly with a view to avoiding unnecessarily long periods of pre-trial detention.*[38]

38 Article LAW.SURR.77, TCA.

© Law Business Research 2021

While proportionality was an existing principle under the United Kingdom's domestic legislation, it was not provided for in the EAW Framework Decision.

As noted above, the role of the CJEU, as the court of last instance in all EAW cases, has been removed. The CJEU has been replaced by the Specialised Committee on Law Enforcement and Judicial Cooperation, which appears to have a mixture of judicial and administrative functions.

Another notable provision in the TCA is that the United Kingdom or EU Member States are permitted to refuse to execute an arrest warrant on the grounds of nationality. States can elect to refuse the extradite their own citizens.[39] Any State wishing to make use of this provision must notify the Specialised Committee. At the time of writing, 10 EU Member States have notified the Committee of their intention to exercise an absolute bar on the extradition of their own nationals to the United Kingdom.[40] A number of other states have attached conditions to the surrender of their own nationals, including a requirement that the requested person's consent is required first. Overall, only a minority of states have not sought to impose some limitation on their own nationals' liability to extradition. It remains to be seen how significant this new stance on surrender will prove, and whether it gives rise to an imbalance in the arrangements between the United Kingdom and the European Union.

While the negotiation of the TCA was under way, all 27 EU member states were pre-emptively added to Schedule A1 of the Extradition (Provisional Arrest) Act 2020, to permit arrest on a request received from a judicial authority in an EU member state without a UK arrest warrant.[41] This action appears to have been taken in anticipation of a 'no deal' Brexit but, in the event, proved unnecessary.

The TCA, which was provisionally approved by the European Union in December 2020 and applied since 1 January 2021 was formally ratified by the European Parliament in April 2021.

In January 2021, judgment was handed down by the High Court in *Polakowski and others*.[42] The Court considered whether there was a lawful basis for the surrender of persons arrested pursuant to EAWs during the transition period (i.e. after the United Kingdom's exit, but prior to the introduction of the TCA). The applicants argued that there was not and that, accordingly, there was no proper basis for their detention (in some cases) or bail conditions (in others). The Court found that the challenge was not arguable and therefore refused permission to appeal for judicial review in each case.

---

39 Article LAW.SURR.83, TCA.

40 Letter to Lord Ricketts, Chair of the EU Security and Justice Sub-Committee, House of Lords, from Kevin Foster MP, Minister for Future Borders and Immigration, 5 March 2021. The EU Member States concerned are Croatia, Finland, France, Germany, Greece, Latvia, Poland, Slovakia, Slovenia and Sweden.

41 https://www.legislation.gov.uk/ukpga/2020/18/enacted/data.pdf.

42 [2021] EWHC Civ 53 (Admin).

© Law Business Research 2021

In reaching its finding, the High Court considered a bewildering array of agreements, statutory instruments and Acts of Parliament. The court concluded that Articles 7, 62(1)(b) and 185 of the Withdrawal Agreement provided that the Framework Decision continued to apply to those cases where arrest on an EAW had taken place before 11 pm on 31 December 2020, and that those provisions of the Withdrawal Agreement were given effect in domestic law by sections 7A to 7C of the European Union (Withdrawal) Act 2018, which confirms that in such cases the 'unmodified' Extradition Act 2003 continues to apply. Additionally, the court confirmed that the CJEU retains jurisdiction over such cases pursuant to Article 86 of the Withdrawal Agreement.

© Law Business Research 2021

33

Monitorships

Robin Barclay QC, Nico Leslie, Christopher J Morvillo, Celeste Koeleveld and Meredith George[1]

33.1 Introduction

In the United States, the past decade has seen a notable increase in the use of independent corporate monitors in connection with the resolution of corporate criminal and regulatory investigations. This trend has also recently found a statutory foothold in the United Kingdom, after a period of sporadic sampling of use of corporate monitorships as a tool in the sentencing armoury. Now, in the wake of the United Kingdom's deferred prosecution agreement regime, it is safe to assume that the appointment of a monitor will increasingly feature in the settlement and disposal of corporate investigations. Although monitors come in many shapes and sizes, they typically help to create and supervise the implementation of compliance and remediation programmes to address the perceived deficiencies that gave rise to the wrongdoing. It is expected that monitors will reduce recidivism for corporate misconduct, benefiting the corporation, its shareholders and the public.

In the United States, monitors have been used in both the civil and criminal contexts, typically in conjunction with a settlement agreement negotiated between the parties to a dispute, and often with the approval and supervision of the courts.[2] Outside the criminal context, monitors have been used as condi-

1 Robin Barclay QC and Nico Leslie are members of Fountain Court Chambers. Christopher J Morvillo and Celeste Koeleveld are partners, and Meredith George is an associate, at Clifford Chance US LLP.

2 In 2014, for instance, the Department of Justice (DOJ) entered into a civil settlement with Citigroup that included a monitorship provision to address Citigroup's false representations to investors regarding its residential mortgage-backed securities. See DOJ press release,

© Law Business Research 2021

tions of settlements between business entities and a wide range of federal and state agencies,[3] as well as international bodies such as the World Bank.[4] Even private litigants have included monitors in their settlement agreements.[5]

Yet the prevalence of monitors as a condition of high-profile corporate criminal resolutions sets the stage for close scrutiny of the practice in the United States and has given rise to congressional hearings, several United States Department of Justice (DOJ) policy enactments, legal challenges and the promulgation of bar association standards. Therefore, this chapter will focus on monitors used in conjunction with the resolution of federal criminal investigations conducted by the DOJ (including, of course, the various United States Attorney's Offices).[6] Because the practice of using monitors is relatively new in the United Kingdom, this chapter will draw parallels and contrasts in UK law and practice where appropriate from the more developed US practice. After briefly discussing the history of corporate monitors in both countries,

---

'Federal and State Partners Secure Record $7 Billion Global Settlement with Citigroup for Misleading Investors About Securities Containing Toxic Mortgages' (14 Jul. 2014). Monitors may also be used in private cases, especially where there are concerns that misconduct may reoccur or an institution's culture needs to be remodelled to ensure future compliance. See, e.g., Athletics Integrity Agreement between the National Collegiate Athletic Association and The Big Ten Conference, and the Pennsylvania State University (29 Aug. 2012), available at www.psu.edu/ur/2012/Athletics_Integrity_Agreement.pdf; NCAA, Former Sen. Mitchell Selected as Penn State Athletics Integrity Monitor (1 August 2012), www.ncaa.org/about/resources/media-center/news/former-sen-mitchell-selected-penn-state-athletics-integrity.

3 The Environmental Protection Agency and Securities and Exchange Commission (SEC) (among many others) also use monitors as part of settlements. See, e.g., Environmental Protection Agency News Release, Duke Energy Subsidiaries Plead Guilty and Sentenced for Clean Water Act Crimes (14 May 2015) (noting that various Duke Energy subsidiaries would be 'monitored by an independent court[-]appointed monitor'); DOJ press release, 'Taiwan-Based AU Optronics Corporation Sentenced to Pay $500 Million Criminal Fine for Role in LCD Price-Fixing Conspiracy' (20 September 2012) (discussing a court-appointed monitor in the antitrust matter against AU Optronics Corporation); Seth Schiesel and Simon Romero, 'WorldCom Strikes a Deal with SEC', *N.Y. Time*s (27 Nov. 2002), www.nytimes.com/2002/11/27/business/worldcom-strikes-a-deal-with-sec.html (discussing WorldCom's settlement with the SEC, which included a monitorship).

4 As part of the World Bank Sanctions Procedures, an independent monitor may be required for parties seeking to remain active with the Bank. World Bank Sanctions Procedures § 9.03 (15 Apr. 2012), available at https://www.worldbank.org/content/dam/documents/sanctions/other-documents/osd/WBGSanctions_Procedures_April2012_Final.pdf.

5 See, e.g., NCAA Appointed Integrity Monitor, supra note 2, at 1. Additionally, monitors are frequently appointed in lawsuits between private plaintiffs and the government. For example, a monitor was appointed as part of the City of New York's settlement with private plaintiffs regarding the police department's discriminatory enforcement of anti-trespassing rules. Memorandum Opinion and Order at 3 n. 8, *Davis v. City of New York*, No. 10 Civ. 0699 (S.D.N.Y. 28 Apr. 2015).

6 Unless otherwise specified, references herein to 'monitors' or 'monitorships' concern DOJ/United States Attorney's Offices (USAO) corporate monitorships.

© Law Business Research 2021

this chapter will analyse certain key issues surrounding the use of monitors in both jurisdictions, including the appointment, roles, supervision and funding of monitors.

33.2 Evolution of the modern monitor

33.2.1 United States

Most monitorships arise as a result of a corporate guilty plea, deferred prosecution agreement (DPA) or non-prosecution agreement (NPA).[7] The DOJ first used DPAs and NPAs in 1993,[8] with the first recognised monitorship following in 1995, in connection with Consolidated Edison's sentencing for disclosure failures following a deadly steam pipe explosion.[9] Spurred on by the collapse of Enron in 2001 and other high-profile instances of corporate misconduct, the US federal government prioritised and increased the investigation and prosecution of corporations. This increase naturally led to a growth in the number of corporate guilty pleas, DPAs and NPAs, and, concomitantly, the rise of monitorships as a condition of settlement.

See Chapters 9 and 10 on co-operating with authorities; and 23 and 24 on negotiating global settlements

As the frequency of monitorships has increased, so too has their level of scrutiny. One of the most controversial aspects of monitorships has been monitor selection. The issue received considerable attention in 2007 when Chris Christie – then the US Attorney for the District of New Jersey – approved, without a bidding process, a contract for a consulting firm founded by his former boss, Attorney General John Ashcroft, to serve as the monitor for medical device company Zimmer Holdings (a contract reportedly worth

7 DPAs and NPAs, while similar in that they are both pretrial settlement options available to the DOJ/USAO, have different collateral consequences for corporate defendants. With a DPA, the DOJ files a criminal information, which under the DPA the DOJ agrees to dismiss after a term of months or years if the corporate defendant complies with all other terms of the settlement. DPAs are, by virtue of being filed with a court, publicly available and therefore subject corporate defendants to adverse public relations and scrutiny. By contrast, with a NPA, the government agrees not to bring charges against the corporate defendant if it complies with the terms of the settlement; NPAs are not required to be disclosed, though they frequently are by the corporate defendant and the DOJ. Because NPAs do not involve the courts, they tend to be far more flexible and desirable for corporate defendants than DPAs.

8 See US Gov't Accountability Off., GAO-10-260T, Prosecutors Adhered to Guidance in Selecting Monitors for Deferred Prosecution and Non-Prosecution Agreements, But DOJ Could Better Communicate Its Role in Resolving Conflicts (2009).

9 See James C McKinley, 'Con Ed Fined and Sentenced to Monitoring for Asbestos Cover-Up', *N.Y. Times* (22 Apr. 1995), www.nytimes.com/1995/04/22/nyregion/con-ed-fined-and-sentenced-to-monitoring-for-asbestos-cover-up.html. Note, the DOJ was not the first government agency to use monitors. Monitors were used as early as 1978 by the SEC. *SEC News Digest*, Issue 80-71 at 3 (10 Apr. 1980), available at https://www.sec.gov/news/digest/1980/dig041080.pdf (noting that in *SEC v. Page Airways, Inc.*, the defendant agreed to 'retain a Review Person to evaluate the methods and procedures followed in this investigation').

© Law Business Research 2021

between US$28 million and US$52 million in monitor fees).[10] Concerns of cronyism, transparency and conflicts of interest led the US Congress to hold an investigative hearing to better understand the appointment.

In the wake of – and likely to quell criticism over – that controversy, the DOJ first issued guidance on the retention and selection of monitors and has since updated its policies three times. The primary materials issued by the DOJ are the following:

- *The Morford Memorandum*: In March 2008, then acting Deputy Attorney General Craig Morford issued a memorandum establishing guidelines and decision-making procedures for the appointment of monitors titled 'Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations'.[11]
- *The Breuer Memorandum*: In June 2009, Assistant Attorney General Lanny A Breuer issued a memorandum titled 'Selection of Monitors in Criminal Division Matters', in which he built on the Morford Memorandum, outlined the terms required in all monitorship agreements and refined the selection and documentation process for monitors.[12]
- *The Grindler Memorandum*: Gary Grindler, then acting Deputy Attorney General, issued a memorandum in March 2010 titled 'Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations', outlining the means by which corporations can reject a monitor's recommendation for being too costly. This guidance was the result of the increasing costs of monitorships and heavy public scepticism about their benefits.[13]
- *The Benczkowski Memorandum*: In October 2018, Assistant Attorney General Brian A Benczkowski issued a memorandum titled 'Selection of Monitors in Criminal Division Matters' that supplemented the guidance provided by the Morford Memorandum. The Benczkowski Memorandum specified, in greater detail, the principles for determining whether a monitor is needed and formalised in many ways the procedures for monitor nomination, selection and approval.[14]

10 Amy Walsh, 'Is the Opaque World of Corporate Monitorships Becoming More Transparent?', *Bus. L. Today* (Dec. 2015), https://www.americanbar.org/groups/business_law/publications/blt/2015/12/08_walsh/.

11 Memorandum from Craig S Morford, Deputy Att'y Gen., to All Component Heads and US Att'ys, Selection and Use of Monitors in Deferred Prosecution Agreements (7 Mar. 2008) (Morford Memorandum).

12 Memorandum from Lanny A Breuer, Assistant Att'y Gen., to All Criminal Div. Personnel, Selection of Monitors in Criminal Division Matters (24 Jun. 2009).

13 Memorandum from Gary G Grindler, Deputy Att'y Gen., Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations (25 May 2010) (Grindler Memorandum).

14 Memorandum From Brian A Benczkowski, Assistant Att'y Gen., Selection of Monitors in Criminal Division Matters (11 Oct. 2018) (Benczkowski Memorandum).

© Law Business Research 2021

> Many defence attorneys read the Benczkowski Memorandum as making corporate monitorships the exception, not the rule, because it directed prosecutors to recommend monitorships only when there is a 'demonstrable need' for them.[15] That will no longer be the case under current Attorney General Merrick Garland, whose Deputy Attorney General, Lisa Monaco, announced in a speech in October 2021 that she was 'rescinding' any 'guidance' that 'suggested that monitorships are disfavored or are the exception'.[16] Going forward, then, we can expect the DOJ to expand the use of corporate monitorships.

As a result of these policies, the DOJ's selection process is arguably the most formalised and transparent of any agency. The DOJ has further increased transparency by publishing a list identifying all corporate monitors actively engaged by companies as a part of their criminal resolutions.[17] Nevertheless, concern over the selection and use of monitors continues, as Deputy Attorney General Monaco also announced the formation of a Corporate Crime Advisory Group to consider these issues, along with corporate recidivism and non-compliance with NPAs and DPAs, and the benchmarks the DOJ should use to measure successful co-operation.[18] The American Bar Association has also weighed in, having promulgated black-letter standards for monitors (the ABA Standards).[19] The ABA Standards address a variety of issues, ranging from the selection and evaluation of monitors to the establishment of monitor work plans, and are 'the culmination of three years of work by an ABA task force in consultation with judges, prosecutors, defence counsel, court personnel, and academics'.[20]

Controversy over monitors has extended to the courtroom, as companies and monitors battle over, *inter alia*, the legality of court-appointed monitors and the scope of the monitor's powers,[21] the monitor selection process and

15 Brian A Benczkowski, Assistant Att'y Gen., Remarks at Global Investigations Review Live New York (8 Oct. 2019), available at https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-global-investigations.

16 Lisa O Monaco, Deputy Att'y Gen., Keynote Address on White-Collar Crime (28 Oct. 2019), available at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

17 See List of Independent Compliance Monitors for Active Fraud Section Monitorship, U.S. Dep't of Justice, https://www.justice.gov/criminal-fraud/strategy-policy-and-training-unit/monitorships (updated 27 May 2021). This public listing also signals the DOJ's view that monitorships will remain a bulwark of its enforcement policies.

18 Lisa O Monaco, Deputy Att'y Gen., Keynote Address on White-Collar Crime, supra note 16. See also infra Section 33.3.

19 ABA Standards for Monitors (standards adopted in August 2015).

20 Walsh, supra note 10. The ABA Standards provide a much more detailed discussion of best practices and considerations for the principles articulated in the DOJ guidance.

21 For example, after a district court in the Southern District of New York found that Apple violated the Sherman Antitrust Act, the court ordered that Apple be subject to a compliance monitor. Apple challenged the appointment both before the district court and, thereafter,

© Law Business Research 2021

the confidentiality of monitor reports,[22] and the costs monitors impose on the company.

See Sections 33.4 and 33.5.5

United Kingdom 33.2.2

As the use of corporate monitors grew in the United States after the collapse of Enron, so UK authorities increasingly recognised the possibility of deploying similar monitorships as part of the resolution of their own corporate criminal investigations.[23] At the outset, this was done *ad hoc* and at the instigation of the relevant investigating authority. By way of example, in 2008 the Serious Fraud Office (SFO) settled civil proceedings against Balfour Beatty arising out of a construction project in Alexandria, Egypt. As part of that settlement, the SFO required the company to accede to 'a form of external monitoring for an agreed period'. This was an early example of the SFO fashioning new tools to remedy perceived corporate governance failings.

Another example was the SFO's successful prosecution of a construction firm, Mabey & Johnson Ltd, in 2009. This was the first-ever successful prosecution of a British company on charges of overseas corruption and breaching United Nations sanctions, and as part of its guilty plea Mabey & Johnson agreed to the appointment of an independent monitor for three years to oversee future conduct. Although this monitorship was approved by the court, Judge Geoffrey Rivlin QC[24] noted that it was likely to prove an expensive exercise and ordered that the costs of the monitor for the first year be capped at £250,000.

Nonetheless, the use of monitorships remained a novelty in the United Kingdom in the absence of a formal statutory footing. Indeed, it even drew notable judicial criticism on occasion. In the case of Innospec Ltd,[25] in which

---

the Second Circuit Court of Appeals, alleging, *inter alia*, that the appointment violated the constitutional separation of powers. See *United States v. Apple Inc.*, 787 F.3d 131, 136 (2d Cir. 2015). As but one example of the alleged constitutional violation, Apple highlighted that after it had moved the district court for a stay of the injunction appointing the monitor, the monitor 'coordinated with the plaintiffs . . . and submitted an affidavit as an integral part of the opposition papers.' Id. at 134, 138. The district court found that the monitor's actions did not evidence the monitor's prejudice against Apple, and though the Second Circuit concurred, it was far more critical of the monitor's conduct: 'It is certainly remarkable that an arm of the court would litigate on the side of a party in connection with an application to the court he serves.' Id. at 138. The Second Circuit also noted that the monitor's submission on behalf of the plaintiffs 'was the opposite of best practice for a court-appointed monitor'. Id.

22 Marieke Breijer, 'ABA London: Keep monitor reports private', Global Investigations Review (13 Oct.2015), http://globalinvestigationsreview.com/article/1024106/aba-london-monitor-reports-private.

23 See further Jo Rickards and Johanna Walsh, 'DPA corporate monitorships in the UK', Global Investigations Review (21 Sep. 2015), http://globalinvestigationsreview.com/article/1018143/dpa-corporate-monitorships-uk.

24 Later and on his retirement as a judge, he became a senior adviser to the Director of the Serious Fraud Office.

25 See *R v. Innospec Limited* [2010] Crim LR 665.

© Law Business Research 2021

a manufacturer was found to have paid substantial bribes to Indonesian and Iraqi officials, the English courts expressly criticised the three-year monitorship regime that had been jointly agreed by the SFO and DOJ as part of a 'global settlement' with the company. This was to be the first-ever US–UK joint monitorship, and illustrated the extent to which the UK investigating authorities were attracted by the US regime in adopting monitorships in the determination of corporate criminal investigations.

However, although the English court was prepared to approve this aspect of the settlement, the case – and in particular the terms of the cross-border determination reached between the parties – was controversial. Most unusually, a senior appellate judge, namely Lord Justice Thomas,[26] was brought in to sit on the case at first instance. He made clear that the court's approval for the appointment of a joint monitorship 'should be no precedent for the future'. In particular, he stated that the dual monitorship risked incurring unnecessary costs, and noted that 'imposing an expensive form of "probation order" seems to me unnecessary for a company which will also be audited by auditors well aware of the past conduct and whose directors will be well aware of the penal consequences of any similar criminal conduct'. In his view, the sums used on such monitoring might have been better allocated to paying fines or compensation. Either way, he made clear that in future 'the request for such an order will have to be fully explained in terms of its cost effectiveness'.[27]

Innospec was widely seen as a setback for bilateral appointment of monitorships and signalled some judicial resistance to the US approach to presenting the court with a sentencing or settlement package to be approved. But, in spite of Lord Justice Thomas's reservations, UK investigating authorities continued to seek and obtain orders for corporate monitorships, and these were included in civil recovery orders agreed between the SFO and both Macmillan Publishers (in 2011) and Oxford Publishing[28] (in 2012). However, the actual and prospective role of monitorships as a tool of corporate compliance has increased substantially since the creation of the DPA regime in the United Kingdom, introduced by the Crime and Courts Act 2013. In light of that legislation, it is now clear that corporate monitorships have an express and permanent statutory place in the UK criminal law calendar of powers and remedies for holding a corporation to account.[29]

Following the passing of that Act, the SFO launched a consultation process in June 2013 to finalise a Code of Practice for the new DPA regime (the Code). The Code was issued on 14 February 2014, and gives close attention to the

26 Lord Chief Justice of England and Wales 2013–2017.

27 *R v. Innospec Limited* [2010] Crim LR 665 at ss. 48–49.

28 See the SFO's press release describing the circumstances of this settlement, which arose because of the publisher's unlawful practices in Kenya and Tanzania: https://www.sfo.gov.uk/2012/07/03/oxford-publishing-ltd-pay-almost-1-9-million-settlement-admitting-unlawful-conduct-east-african-operations/.

29 See Crime and Courts Act 2013, Schedule 17, Part I, s.5(3)(e).

© Law Business Research 2021

role and duties of corporate monitors. Although such monitorships are not a mandatory feature of the new regime, the focus on monitoring in the Code is a powerful indication of the role that UK authorities expect them to play in the future. The Code also sets out a detailed framework for the appointment of monitors, the costs and terms of the monitorship, and the areas that the monitor may be expected to supervise or restructure.[30]

The SFO's first application for a DPA was approved by a senior appellate judge, Sir Brian Leveson, then President of the Queen's Bench Division, on 30 November 2015.[31] The DPA involved Standard Bank Plc, which was the subject of bribery charges relating to multimillion-dollar payments made by a former sister company in Tanzania. As part of the agreed DPA, Standard Bank agreed to submit, at its own expense, to an 'independent review of its existing internal anti-bribery and corruption controls, policies and procedures regarding compliance with the Bribery Act 2010 and other applicable anti-corruption laws'.[32] The independent reviewer appointed was PricewaterhouseCoopers LLP. In his judgment approving the DPA, Leveson P made a number of observations about the difference between the DPA regimes in the United Kingdom and the United States, noting that '[i]n contra-distinction to the United States, a critical feature of the statutory scheme in the UK is the requirement that the court examine the proposed agreement in detail, decide whether the statutory conditions are satisfied and, if appropriate, approve the DPA'. In particular, he observed that the court will only approve a DPA if it is fair, reasonable and proportionate in all the circumstances, but that it will typically consider this question in private so as not to prejudice any potential prosecution in the event of an adverse decision.[33] In the case of Standard Bank, he declared himself fully satisfied that the DPA was in the interests of justice.[34]

Following the high-profile *Standard Bank* case, the SFO soon made a second successful application for a DPA, approved by Leveson P on 6 July 2016.[35] The company, Sarclad Limited, which originally could not be named because of parallel legal proceedings, pleaded guilty to charges of conspiracy to corrupt. The DPA provided that Sarclad would undertake a review of its internal compliance controls, and that its chief compliance officer would prepare a report for submission to the SFO on its anti-corruption policies and their implementation, to be submitted within 12 months of the DPA and then annually for the DPA's duration.[36] Although it is not known why this approach was taken by the SFO, it seems likely that it was because the company in question was

30 See, in particular, DPA Code of Practice, para. 7, headed 'Terms'.

31 See SFO press release, https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/.

32 Id.

33 See *SFO v. Standard Bank Plc* [2016] Lloyd's Rep FC 102 at para. 2.

34 Id. at para. 22.

35 See SFO press release, https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/.

36 See *SFO v. XYZ Ltd*, unreported, 24 June 2016, at para. 64.

© Law Business Research 2021

relatively small and the appointment of a full-time monitor would have been unduly financially onerous. Again, this would appear to demonstrate the flexibility with which UK authorities are now prepared to apply monitoring tools to fashion bespoke remedies for corporate wrongdoing.

Another example is the DPA agreed between the SFO and Tesco Stores Ltd, the supermarket conglomerate, on 28 March 2017 in respect of accounting irregularities. Deloitte was appointed to a monitoring role to review and report on Tesco's controls and governance in respect of the recognition of commercial income.[37] This suggests an ever wider role for corporate monitorships in the United Kingdom, which may be imposed in contexts beyond international bribery and corruption. However, the touchstone for the appropriateness of a monitorship is always likely to be how the corporate has responded to allegations of wrongdoing: in the DPA agreed between the SFO and Serco Geografix Ltd,[38] dated 2 July and judicially approved on 4 July 2019, the SFO was satisfied that an undertaking of ongoing co-operation by its parent and a far-reaching corporate renewal programme were sufficient to make a monitorship unnecessary. The SFO adopted a similar approach in its recent DPA with Airbus SE, judicially approved on 31 January 2020, and agreed that a monitorship was not required in the light of what the reviewing judge described as 'significant changes to [the company's] internal processes'[39] and also because the Agence Française Anticorruption was appointed to oversee improvements to Airbus's compliance arrangements in any event. By contrast, in the still more recent DPA agreed between the SFO and G4S Care and Justice Services, approved by the courts on 17 July 2020, the SFO adopted an intermediate position. While it agreed not to impose a formal monitorship on the respondent company in the light of internal governance changes, it nonetheless insisted on the appointment of an external reviewer 'to review and report on the compliance measures being taken' by the company and its subsidiaries.[40] The new regime was described by Justice Davis in the following terms: 'The intensity of the external scrutiny as set out in the DPA is greater than in any previous DPA. This is necessary and appropriate given the exposure of both G4S C&J and the parent company to government contracts. Equally, it is an important factor in providing reassurance to the SFO, to relevant government

37 See FCA Final Notice to Tesco Stores Ltd dated 28 March 2017, at s. 4.10. The DPA was later approved by Leveson P at a hearing on 10 April 2017 and reporting restrictions were lifted in January 2019 following the acquittal of three individuals, https://www.sfo.gov.uk/2019/01/23/deferred-prosecution-agreement-between-the-sfo-and-tesco-published/.

38 See the DPA between Serco Geografix Ltd and the Serious Fraud Office, 2 July 2019, https://www.sfo.gov.uk/download/deferred-prosecution-agreement-serco-geografix-ltd-sfo/ at para. 5(ii)(b)(i) and (iii) and *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518.

39 See *SFO v. Airbus SE*, unreported, 31 January 2020 at para. 79, *per* Dame Victoria Sharp P.

40 See *SFO v. G4S Care and Justice Services (UK) Ltd*, unreported, 17 July 2020 at para. 43, *per* Davis J.

© Law Business Research 2021

departments and to the wider public that both companies have proper controls in place to ensure the integrity of their accounting and governance processes. The DPA will last for three years, during which period the compliance measures will continue and will be reviewed.[41] This is an indication of the flexible way in which the SFO approaches ensuring compliance.

In light of these developments, where the circumstances and interests of justice require it, the use of corporate monitorships looks set to increase in the United Kingdom, and a greater convergence with US practice can be expected. This is all the more so given the appointment of Lisa Osofsky, a former deputy general counsel of the FBI and a monitor in private practice, as Director of the SFO in 2018. In a keynote speech on 17 October 2018, Ms Osofsky highlighted the differences between the UK and US regimes in respect of corporate prosecutions and DPAs but indicated that the SFO may take a more interventionist approach in future. Above all, she stressed that the SFO 'will want assurance that companies are doing everything they can to ensure the crimes of the past won't be repeated'.[42] In that context, and subject to the terms of the Code, the UK authorities' approach to the appointment and conduct of corporate monitors is ever more likely to follow the lead of the United States in the coming years. Although in the recent DPAs reached with Amec Foster Wheeler Energy Limited (AFWEL) in June 2021[43] and two yet to be identified UK-based companies in July 2021,[44] the SFO agreed to corporate undertakings to provide it with annual reports on corporate remedial works and compliance enhancements during the term of the DPAs instead of monitors (the court in *AFWEL* noting that the undertaking extended beyond AFWEL to the whole Wood Group and wider than other orders the court could impose, and was tailored to the facts of the case).[45]

See Chapter 23 on negotiating global settlements

Circumstances requiring a monitor 33.3

In general, the DOJ assesses the need for the appointment of a monitor based on whether the corporation is capable of remediating, or has already remediated, its past wrongdoings without the assistance of a monitor, and whether the

41 See also the words of the Director of the SFO in a press release dated 17 July 2020: 'G4S C&J and its parent company, G4S plc – a significant government supplier – will be subjected to unprecedented, multi-year scrutiny and assurance', at https://www.sfo.gov.uk/2020/07/17/sfo-receives-final-approval-for-dpa-with-g4s-care-justice-services-uk-ltd/.

42 Keynote speech on Future SFO Enforcement at New York University School of Law (17 Oct. 2018), https://wp.nyu.edu/compliance_enforcement/2018/10/16/director-of-the-serious-fraud-office-lisa-osofsky-keynote-on-future-sfo-enforcement/.

43 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep. FC Plus 27.

44 See https://www.sfo.gov.uk/2021/07/20/sfo-secures-two-dpas-with-companies-for-bribery-act-offences/.

45 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep. FC Plus 27.

© Law Business Research 2021

DOJ believes there is a risk of recidivism. That, in turn, often translates into an enquiry of 'tone at the top' – whether, *inter alia*, management was involved in the criminal conduct, was negligent in failing to implement a proper compliance programme, fostered a culture that bred non-compliance with ethical and legal duties, and, critically, self-reported the misconduct to the DOJ.[46]

See Chapters 3 and 4 on self-reporting to authorities

The DOJ places significant weight on a company's decision to self-report. The importance of self-reporting was demonstrated in the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, announced on 29 November 2017,[47] and most recently updated in November 2019.[48] The Corporate Enforcement Policy states: 'When a company has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated . . . there will be a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender.'[49] Significantly, the DOJ has recently signalled its intent to apply the Corporate Enforcement Policy's principles to other white-collar matters,[50] further emphasising the value it places on self-disclosure. Therefore, with increased self-reporting, it is reasonable to expect that monitorships will decline.[51] However, it is still unclear how the Biden administration will handle self-disclosure and monitorships, and the DOJ's new policies are likely to result in more monitorships than during the Trump administration.

See Chapters 3 and 4 on self-reporting to authorities

In addition to self-reporting, the DOJ considers the effectiveness of a company's compliance programme. Under the FCPA Corporate Enforcement Policy, '[i]f a criminal resolution is warranted', the DOJ 'generally will not require appointment of a monitor if a company has, at the time of resolution, implemented an effective compliance program'.[52] Recently, the DOJ has reiterated the importance of an effective compliance programme in its monitor decision-making through updated guidance to prosecutors on the 'Evaluation

46 See 'Is a Corporate Monitor Necessary?', Corp. Crime Rep. (8 May 2013), www.corporatecrimereporter.com/news/200/isamonitornecessary05082013/.

47 Rod Rosenstein, Deputy Attorney General, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (29 Nov. 2017).

48 Justice Manual, US Dep't of Justice, § 9-47.120 (last updated November 2019).

49 Id.

50 Kelly Swanson, 'DOJ expanding use of FCPA declination policy principles', Global Investigations Review (2 Mar. 2018), https://globalinvestigationsreview.com/article/1166274/doj-expanding-use-of-fcpa-declination-policy-principles.

51 Deputy Attorney General Sally Quillian Yates's September 2015 memorandum, 'Individual Accountability for Corporate Wrongdoing' [Yates Memorandum], reinforces the importance of internal risk assessment and compliance monitoring. As promulgated, the Yates Memorandum requires early and complete self-reporting if a corporation wishes to obtain co-operation credit. Corporations are thus highly incentivised to self-report.

52 Justice Manual, US Dep't of Justice, § 9-47.120 (last updated November 2019).

© Law Business Research 2021

of Corporate Compliance Programs',[53] and the release of the Second Edition of its Resource Guide to the FCPA.[54] Both updates expressly incorporate and reflect the principles in the Benczkowski Memorandum.[55] The Benczkowski Memorandum provided additional guidance to the Morford Memorandum, which offered two broad considerations to guide prosecutors when deciding when a monitor is appropriate: '(1) the potential benefits that employing a monitor may have for the corporation and the public, and (2) the cost of a monitor and its impact on the operations of a corporation."[56] Because of the breadth of these considerations, the Benczkowski Memorandum clarified that when assessing 'potential benefits' of the monitorship, one must consider, among other factors: (1) whether the misconduct involved the manipulation of books and records or the exploitation of an inadequate compliance programme, (2) the pervasiveness of the misconduct across the business organisation and the degree of its facilitation by senior management, (3) investments by the corporation to improve its compliance programme and internal controls, and (4) whether these remedial improvements had been tested to detect or prevent future similar misconduct.[57] Ultimately, the Benczkowski Memorandum laid down the principle adopted in the Corporate Enforcement Policy: 'Where a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not likely be necessary.'[58] These considerations must be weighed in light of case-specific factors, including the particular regions and industries involved.[59]

Notably, the Benczkowski Memorandum also states that the Criminal Division of the DOJ should only favour the imposition of a monitor when there is a 'demonstrated need for, and a clear benefit' from the monitorship relative to the 'projected costs and burdens' it will create.[60] As noted earlier,

53 Evaluation of Corporate Compliance Programs, U.S. Dep't of Justice (Jun. 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.

54 A Resource Guide to the US Foreign Corrupt Practices Act, Second Edition, U.S. Dep't of Justice and U.S. Securities Exch. Comm'n (Jul. 2020), https://www.justice.gov/criminal-fraud/file/1292051/download. The Second Edition was the first substantive update since the Resource Guide's publication in 2012.

55 Id. at 73–74; Evaluation of Corporate Compliance Programs, supra note 53, at 1, 15.

56 Morford Memorandum, supra note 11, at 2.

57 Benczkowski Memorandum, supra note 14, at 2.

58 Id.

59 Commentators have noted that monitorships may be appropriate where companies have faced significant cybersecurity breaches, such as Yahoo!, where a recent breach resulted in the theft of data from more than one billion accounts. See Jacob S Frenkel and Justin L Root, 'Analysis: Cyber-Monitoring: The Next Frontier' (7 Mar. 2017), http://www.dickinson-wright.com/-/media/files/news/2017/03/analysis-cyber-monitoring-the-next-frontier.pdf?la=en. In such cases, the severity of the breach and the complexity of the problem are two factors that may well have a bearing on a decision to impose a monitor.

60 Benczkowski Memorandum, supra note 14, at 2. See also Deputy Assistant Att'y Gen. Matthew S Miner Remarks at the 29th Annual National Institute on Health Care Fraud, New Orleans

© Law Business Research 2021

the defence bar read this as a marked shift away from monitorships, a reading that current Deputy Attorney General Lisa Monaco has now explicitly disavowed.[61] Benczkowski himself addressed this impression in a keynote address in April 2019: 'Put simply, this guidance was not meant to do away with monitors – it was meant to focus our prosecutors' determination on the appropriate factors so that monitors are imposed only where necessary and under the terms and scope that is appropriate for that given case.'[62] In the wake of this guidance, the DOJ has entered into plea agreements requiring tailored monitorships to address the issues at hand, as demonstrated by Walmart's recent settlement, discussed further below. The DOJ also seems willing to adopt quasi-monitorship structures, where a full-blown monitorship is ill-suited.[63] At the same time, some prominent settlements of corporate criminal liability, most notably that of the DOJ with Goldman Sachs regarding its involvement

(9 May 2019), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-gives-remarks-29th-annual-national (noting the 'bottom line' is that the 'Criminal Division should favor the imposition of a monitor only where there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to the projected costs and burdens').

61 Lisa O Monaco, Deputy Att'y Gen., Keynote Address on White-Collar Crime, supra note 16. See infra Section 33.3.

62 Assistant Att'y Gen. Brian A Benczkowski Keynote Address at the Ethics and Compliance Initiative 2019 Annual Impact Conference, Dallas, Texas, 30 April 2019, https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-keynote-address-ethics-and; see also Adam Dobrik, 'Criminal division chief plays down talk of monitorship demise', Global Investigations Review (8 March 2019), available at https://globalinvestigationsreview.com/article/jac/1181316/criminal-division-chief-plays-down-talk-of-monitorship-demise (quoting Benczkowski: 'There were many who thought [the Benczkowski Memorandum] reflected a sort of Shakespearean policy of first, let's kill all the monitors. But that's not what it was meant to do. . . . In fact, it was meant to provide greater clarity both to companies but also to our prosecutors to ensure that when they do recommend the appointment of a monitor that they are doing so for the right reasons and with the right scope.').

63 In July 2019, Facebook entered into a record-breaking US$5 billion settlement with the Federal Trade Commission (FTC) and DOJ over data privacy claims. The consent order requires Facebook to appoint an 'independent assessor', chosen by Facebook but approved by the FTC and DOJ, to monitor its compliance with the terms of the order for a 20-year term. Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief and Memorandum in Support at 5, *United States v. Facebook, Inc.*, No. 19-cv-02184 (D.D.C. 24 Jul. 2019); Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 4, *United States v. Facebook, Inc.*, No. 19-cv-02184 (D.D.C. 24 Jul. 2019). The independent assessor must, *inter alia*, conduct an initial and biennial assessment of Facebook's privacy programme, to be shared with the FTC and DOJ, and attend quarterly meetings with a newly established independent privacy committee of the board of directors, both with and without management present, to discuss privacy risks. Decision and Order at VIII.F, X.A.5, *In re Facebook, Inc.*, Docket No. C-4365 (F.T.C. 24 Jul. 2019).

© Law Business Research 2021

in the 1MDB scandal,[64] did not involve the imposition of a monitor, presumably because Goldman Sachs successfully argued that it already had an effective compliance programme in place.

Note that even corporations registered under the laws of a foreign country are subject to DOJ monitorships, provided the United States has jurisdiction over the corporation's misconduct. Indeed, in recent years in the United States, monitors have been imposed on foreign offenders with increased frequency, many in relation to alleged violations of the FCPA.[65] Notably, nine of the 10 largest FCPA settlements to date involve non-US companies and six of them required a corporate monitor.[66]

---

64 https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.

65 See SEC press release, 'VimpelCom to Pay $795 Million in Global Settlement for FCPA Violations' (18 Feb. 2016), https://www.sec.gov/news/pressrelease/2016-34.html (noting that the SEC imposed a monitor on Dutch company VimpelCom as part of the parties' settlement to resolve VimpelCom's FCPA violations); Independent Monitor of Takata and the Coordinated Remedy Program, Takata Monitor, www.takatamonitor.org/ (Japanese company Takata agreeing to a monitor for its manufacture and sale of ammonium nitrate airbags in connection with its settlement with the US National Highway Traffic Safety Administration).

66 (1) Airbus Agrees to Pay over $3.9 Billion in Global Penalties [$2.09 Billion with the DOJ] to Resolve Foreign Bribery and ITAR Case, U.S. Dep't of Justice (31 Jan. 2020), https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case (settlement included monitorship); (2) Ericsson Agrees to Pay Over $1 Billion to Resolve FCPA Case, U.S. Dep't of Justice (6 Dec. 2019), https://www.justice.gov/opa/pr/ericsson-agrees-pay-over-1-billion-resolve-fcpa-case (settlement included monitorship); (3) Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter into Resolutions of $850 Million with the Department of Justice for Paying Bribes in Uzbekistan, U.S. Dep't of Justice (7 Mar. 2019), https://www.justice.gov/opa/pr/telia-company-ab-and-its-uzbek-subsidiaryenter-global-foreign-bribery-resolution-more-965 (settlement included monitorship); (4) VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme, U.S. Dep't of Justice (18 Feb. 2016), https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million (settlement included monitorship); (5) Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges, U.S. Dep't of Justice (22 Dec. 2014), https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery (settlement included monitorship); (6) Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines, U.S. Dep't of Justice (15 Dec. 2008), https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html (settlement included monitorship); (7) Petróleo Brasileiro S.A. – Petrobras Agrees to Pay More Than $850 Million for FCPA Violations, U.S. Dep't of Justice (27 Sep. 2018); (8) Société Générale S.A. Agrees to Pay $860 Million in Criminal Penalties for Bribing Gaddafi-Era Libyan Officials and Manipulating LIBOR Rate, U.S. Dep't of Justice (4 Jun. 2018), https://www.justice.gov/opa/pr/soci-t-g-n-rale-sa-agrees-pay-860-million-criminal-penalties-bribing-gaddafi-era-libyan; (9) Telia Company AB and Its Uzbek Subsidiary

© Law Business Research 2021

Similar tests are applied in the United Kingdom.[67] The Code sets out some important considerations for the appointment of a monitor, including whether the company already has a 'genuinely proactive and effective corporate compliance programme' and whether the appointment would be fair, reasonable and proportionate in all the circumstances.[68]

As in the United States, there is likely to be a particular focus on the degree of culpability of the management, especially if that management is still in place. Where the management has been entirely replaced, or where misconduct has been self-reported, there may be less need for an extended monitorship (see, for example, the observations made by the court in *Innospec*).[69] Moreover, and again in light of the comments in *Innospec*, the United Kingdom is likely to apply a special focus to matters of cost-effectiveness. Much is likely to turn on an analysis of what is fair, reasonable and proportionate in the circumstances of the specific proposed monitorship.

33.4 Selecting a monitor

The selection of the monitor is often the most controversial aspect of monitorships, as claims of cronyism abound. As outlined by the Morford Memorandum, the government should ensure that the monitor is highly qualified, does not have any conflict of interests (either with the government or the corporation), and will instil public confidence in the monitorship process.[70] The Benczkowski Memorandum attempts to standardise the selection process by creating a Standing Committee on the Selection of Monitors (the Standing Committee).[71] The Standing Committee comprises (1) the Deputy Assistant Attorney General with supervisory responsibility for the Fraud Section, who also serves as the chair of the Standing Committee, (2) the Chief of the Fraud Section (or other relevant Section), and (3) the Deputy Designated Agency Ethics Official for the Criminal Division.[72] To the extent any of these individuals are unable to serve, they may designate a replacement. To the extent further replacements are necessary for any given case, the chair of the Standing

Enter Into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan, U.S. Dep't of Justice (21 Sep. 2017), https://www.justice.gov/opa/pr/telia-company-ab-and-its-uzbek-subsidiary-enter-global-foreign-bribery-resolution-more-965.

67 See https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/evaluating-a-compliance-programme/ (especially Principle 6 and accompanying Guidance).

68 See, in particular, DPA Code of Practice, para. 7.11.

69 *R v. Innospec Limited* [2010] Crim LR 665 at ss.48–49.

70 Morford Memorandum, supra note 11, at 3.

71 Benczkowski Memorandum, supra note 14, at 5.

72 Id. at 3–4.

© Law Business Research 2021

Committee may appoint them.[73] The Standing Committee is expected to continue under Attorney General Merrick Garland.

The ABA Standards suggest that both parties 'have a significant role in the selection process', enumerate multiple selection criteria, and outline mandatory and potential exclusions.[74] To this end, the Benczkowski Memorandum provides for the corporation to recommend three qualified candidates through a written proposal. The proposal should provide a description of the candidates' qualifications and credentials; certification that the candidates have no current or future affiliation with the corporation and no conflict of interest in serving as the monitor; and a statement identifying the corporation's first choice to serve as monitor.[75] The Criminal Division attorneys handling the matter and their supervisors assess the candidates according to the factors detailed in the Benczkowski Memorandum, and recommend one of the candidates to the Standing Committee.[76] The Standing Committee votes on the recommended candidate and forwards their acceptance or rejection to the Assistant Attorney General of the Criminal Division, who must review and consider the recommendation (and cannot unilaterally accept or veto it).[77] Pursuant to this process, the Assistant Attorney General may request additional information from the Standing Committee and may interview the proposed candidate. He or she then notes disagreement or concurrence with the proposed candidate before sending the decision to the next step.[78] As a further layer of review, all monitor candidates selected pursuant to DPAs, NPAs and plea agreements must be approved by the Office of the Deputy Attorney General.[79]

One issue with past selection methods is that they have not resulted in a diverse monitor pool.[80] For example, between 2004 and 2018, only three women and three non-white attorneys (all male) have been chosen by the DOJ to serve as FCPA monitors, even though there have been more than 45 settlements involving FCPA monitors during the same period.[81] The DOJ appears

73 Id. at 3.

74 ABA Standards for Monitors, §§ 24-2.1; 24-2.4.; 24-2.4(3)–(4).

75 Benczkowski Memorandum, supra note 14, at 5.

76 Id. at 5–7. Factors for consideration include the candidates' credentials, experience and expertise, degree of objectivity and independence from the corporation, adequacy of resources to discharge responsibilities and any other relevant factors, as determined by the reviewing attorneys.

77 Id. at 7–8.

78 Id.

79 Id. at 8.

80 Dylan Tokar, 'Women and minorities lose out in FCPA monitor selection process', Global Investigations Review (1 Feb. 2018), https://globalinvestigationsreview.com/article/jac/1153265/women-and-minorities-lose-out-in-fcpa-monitor-selection-process.

81 Id. These statistics were made available after a court battle fought by a Global Investigations Review reporter. The reporter filed a lawsuit in December 2016, seeking the names of monitor candidates considered for 15 companies involved in compliance investigations, and the names of the DOJ attorneys involved in the selection process. In March 2018, he

© Law Business Research 2021

to be alive to this issue. On 30 April 2018, the DOJ and a US-based subsidiary of Panasonic entered into a DPA to resolve FCPA violations, under which the company agreed to a two-year monitorship.[82] The DOJ included a provision in the DPA that stated: 'Monitor selections shall be made in keeping with the Department's commitment to diversity and inclusion.'[83] The DPA also includes various provisions that enable the DOJ to broaden the group of candidates from which it will select the monitor.[84] While the DOJ cannot consider non-merit-based factors such as race and gender when choosing the most-qualified candidate, these provisions help ensure that the pool from which the DOJ makes its selection is more diverse. A DOJ spokesperson indicated that the above quoted language was added to the Criminal Division's standard agreements in January 2017,[85] and therefore it will likely be a recurring feature in the department's DPAs. It remains to be seen whether the protocols established by the Benczkowski Memorandum will help create a more diverse monitor pool. However, the one corporate monitorship established so far in 2021 has a woman as one of its corporate monitors, sparking some optimism for future diversity.[86]

There is also an open question as to judicial oversight of the selection process. In March 2017, the DOJ reached a plea agreement with ZTE for conspiring to violate export control laws, under which ZTE would plead guilty

---

prevailed, when the District Court for the District of Columbia ruled that the public's interest in learning the candidates' identities outweighed the government's privacy interest. See *Tokar v. U.S. Dep't of Justice*, No. 16-2410, 2018 WL 1542320 (D.D.C. 29 Mar. 2018); Jody Godoy, 'DOJ Sued by Reporter Seeking FCPA Monitor Records', *Law360* (9 Dec. 2016), https://www.law360.com/articles/871052/doj-sued-by-reporter-seeking-fcpa-monitor-records. Recently, that reporter also secured a settlement for attorneys' fees from the DOJ, bringing the nearly five-year public records battle to a close. Courtney Douglas, Reporters Committee reaches settlement with Justice Department after 5-year FOIA battle, Reporters Committee (17 July 2020), https://www.rcfp.org/tokar-doj-foia-settlement/.

82 Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp. (30 Apr. 2018), available at https://www.justice.gov/opa/press-release/file/1058466/download.

83 Id. at 12.

84 Id. ('If the Fraud Section determines, in its sole discretion, that any of the candidates are not, in fact, qualified to serve as the Monitor, or if the Fraud Section, in its sole discretion, is not satisfied with the candidates proposed, the Fraud Section reserves the right to request that the company nominate additional candidates. In the event the Fraud Section rejects any proposed monitors, the Company shall propose additional candidates . . . so that three qualified candidates are proposed.').

85 Clara Hudson, 'Lawyers laud criminal division's diversity provision for monitors', Global Investigations Review (3 May 2018), https://globalinvestigationsreview.com/article/jac/1168991/lawyers-laud-criminal-divisions-diversity-provision-for-monitors.

86 See List of Independent Compliance Monitors for Active Fraud Section Monitorship, U.S. Dep't of Justice, https://www.justice.gov/criminal-fraud/strategy-policy-and-training-unit/monitorships (updated 27 May 2021) (stating that the corporate monitors established in 2021 for The Bank of Nova Scotia are Rita Molesworth and William Stellmach).

© Law Business Research 2021

to three criminal charges and, as part of the sentence, be subject to a three-year monitorship, with the monitor selected by the DOJ 'in its sole discretion' from a pool of candidates proposed by ZTE.[87] In an unprecedented move, the court overseeing the matter – the District Court for the Northern District of Texas – required the parties to amend the terms of the plea agreement to impose a monitor of its own selection and to increase judicial oversight over the monitorship.[88] Specifically, the plea agreement was amended to state that James M Stanton would be appointed as ZTE's monitor,[89] that 'the Monitor is a *judicial adjunct* pursuant to Federal Rule of Civil Procedure 53'[90] and that '[a]ll reports, submissions, or other materials encompassed by this agreement will be filed [with the Court]'.[91] The appointment of Mr Stanton, a lawyer in private practice and a former Texas state judge, was seen by some as particularly unusual given his lack of monitorship experience.[92] Notably, ZTE's monitorship was imposed as part of a plea agreement subject to court review and approval. Accordingly, the court had the opportunity to amend the terms of the agreement before approving the plea. It remains to be seen whether courts will take as active a role in crafting the terms of monitorships imposed as part of DPAs and NPAs, which do not require the court's approval.[93]

87 Plea Agreement at Attachment A ¶¶ 1–2, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 7 Mar. 2017) ('[T]he Company will propose to the Department three candidates to serve as the Monitor. . . . The Department retains the right, in its sole discretion, to accept or reject the Monitor candidates proposed by the Company.').

88 The process for selecting the monitor and the terms of the monitorship were outlined in Attachment A to the Plea Agreement. The court subsequently amended Attachment A but left the remainder of the Plea Agreement intact. See Attachment A (Modified) Independent Corporate Compliance Monitor, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 Mar. 2017). See also Rearraignment Hearing, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 Mar. 2017) ('Here's what the agreement is as I understand it: It would be a sentence of three years' probation on each count, to run concurrently, with an independent corporate compliance monitor appointed by me, by the Court, which is – I have chosen Mr. James Stanton; or if something happens to him or if I choose to change, that would be who it would be, as set out in Attachment A as modified today.').

89 Attachment A (Modified) Independent Corporate Compliance Monitor ¶ 1, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 Mar. 2017) ('ZTE Corporation . . . agrees to engage James M. Stanton as an independent corporate monitor').

90 Id. ¶ 6 (emphasis added).

91 Id. ¶ 13.

92 See Sue Reisinger, 'In Rare Move, Judge Imposes Own Monitor in ZTE Plea Deal', *The American Lawyer* (29 Mar. 2017), http://www.americanlawyer.com/id=1202782436926/In-Rare-Move-Judge-Imposes-Own-Monitor-in-ZTE-Plea-Deal?mcode=0&curindex=0&curpage=ALL (noting that James Stanton is a civil and personal injury lawyer with no prior experience of acting as a monitor and no significant criminal experience, albeit, per his resume, he has served as a special master and arbitrator in six civil cases).

93 See *United States v. Fokker Services BV*, 818 F.3d 733, 741 (D.C. Cir. 2016).

© Law Business Research 2021

In the United Kingdom, a slightly different appointment procedure has been laid down by the Code. As part of the negotiations surrounding a DPA in the United Kingdom, the company must provide the prosecuting authority and the court with details of three potential monitors, including their qualifications, their estimated costs and any links with the relevant company. The company should then indicate their preferred monitor of the three, stating the reasons for their preference. This choice will ordinarily be accepted by the prosecuting authority and court, except where a conflict of interest or a lack of relevant experience has been identified.[94]

In terms of eligibility, the monitor must be independent from the company, and thus former employees, clients and close acquaintances are likely ineligible. Additionally, as the requirements of the monitorship will differ case by case, the monitor should be selected based on how well his or her qualifications pair with the requirements of the relevant monitorship.[95] For example, the DPA between the DOJ and Panasonic lists the minimum contemplated qualifications of a monitor as (1) 'sufficient independence' from Panasonic, (2) 'demonstrated expertise with respect to the FCPA and other applicable anti-corruption laws, including experience counseling on FCPA issues', (3) 'experience designing and/or reviewing corporate compliance policies, procedures and internal controls, including FCPA and anti-corruption policies, procedures, and internal controls', and (4) 'ability to access and deploy resources necessary to discharge the Monitor's duties' under the agreement.[96]

In global settlements, both US and UK authorities increasingly see the value of appointing a monitor experienced in the laws of the relevant jurisdiction.[97] Although the Morford Memorandum suggests that non-attorney experts 'such as accountants, technical or scientific experts, and compliance experts' may be better qualified for certain monitorships, in practice, monitors in the United States are predominantly lawyers, and often have prosecutorial experience.[98]

---

94 See, in particular, DPA Code of Practice, paras. 7.15–7.17.

95 See Benczkowski Memorandum, supra note 14, at 2.

96 Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp., supra note 72, at 11–12.

97 See infra notes 126–128 and accompanying text discussing Rolls-Royce's monitor, British lawyer Lord Gold.

98 One study found that half of all monitors appointed in connection with DPAs and NPAs since 2001 have been former prosecutors, leading some critics to describe the monitoring industry as a 'full employment act for former federal prosecutors'. See Alison Frankel, 'DOJ should end secret selection process for corporate watchdogs', Reuters Blog (14 Jul. 2014), http://blogs.reuters.com/alison-frankel/2014/07/14/doj-should-end-secret-selection-process-for-corporate-watchdogs/; Steven Davidoff Solomon, 'In Corporate Monitor, a Well-Paying Job But Unknown Results', *NY Times: Dealbook* (15 Apr. 2014), http://dealbook.nytimes.com/2014/04/15/in-corporate-monitor-a-well-paying-job-but-unknown-results/. As but one recent example, the former Deputy Chief in the Fraud Section of the Criminal Division of the DOJ was appointed to serve as a monitor for Odebrecht as part of its guilty plea for FCPA violations. See Jody Godoy, 'DOJ Taking $24m Haircut on

© Law Business Research 2021

Note, however, the requirements of the monitorship can evolve over its duration, and the appointed monitor may prove incompatible with the corporation. In that case, the government may replace the monitor, who is also free to resign. As one example of a rather tumultuous monitorship, Western Union went through four monitors as part of a 2010 settlement for failing to comply with anti-money laundering laws.[99]

To avoid such situations, third-party organisations have devoted themselves to promoting the use, quality and efficiency of monitors.[100] For example, the International Association of Independent Corporate Monitors – whose board is itself composed of many former monitors – offers resources and training to professionals, and has established a Code of Professional Conduct to serve as a template for best standards and practices.[101]

The role of the monitor 33.5

Scope of the monitorship 33.5.1

The scope of the monitorship should be tailored to the circumstances of each case, with the ultimate goal of reducing the risk of recurrence of the corporation's misconduct.[102] Therefore, the monitor's role should normally include a mandate for oversight, review and proposed modification of a company's compliance programme to facilitate rehabilitation of existing misconduct and deterrence of future wrongdoing.[103] Accordingly, the monitor may be required to assist

---

Odebrecht's $2.6B FCPA Fine', *Law360* (12 Apr. 2017), https://www.law360.com/articles/912549/doj-taking-24m-haircut-on-odebrecht-s-2-6b-fcpa-fine; Biography of Charles E Duross, Morrison Foerster, https://www.mofo.com/people/charles-duross.html.

99 Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 Aug. 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917. On 9 June 2017, a court accepted the monitor's final report, thereby ending Western Union's monitorship. See The Western Union Company, Form 8-K, filed 9 June 2017.

100 International Association of Independent Corporate Monitors, 'About Us', at http://iaicm.org/about-independent-corporate-monitors/ (describing the mission/purpose of the organisation and discussing the Code of Professional Conduct) (last accessed 24 August 2021).

101 Id. (touting its members as having the 'breadth and depth of relevant skills, knowledge, and experience, together with reputation of character, to effectively serve as [monitors]'). See also Thomas Fox, 'IAICM Shine a Light on Corporate Monitors', JD Supra, 8 March 2017, http://www.jdsupra.com/legalnews/iaicm-shine-a-light-on-corporate-85994/. Membership is comprised of a 'distinguished panel of current and former corporate monitors, retired judges, and one former FBI agent'.

102 Morford Memorandum, supra note 11, at 5.

103 See, e.g., Dep't of Justice Deferred Prosecution Agreement with Avon Products, Inc., 15 December 2014, available at https://www.sec.gov/Archives/edgar/data/8868/000000886814000073/exhibit992dpa.htm ('the Monitor will evaluate, in the manner set forth below, the effectiveness of the internal accounting controls, record-keeping, and financial reporting policies and procedures of the Company as they relate to the Company's current and ongoing compliance with the FCPA').

© Law Business Research 2021

with structural changes, as well as help alter corporate culture and normative expectations.[104] In the United Kingdom, a list of items and procedures that the monitor may wish to consider as part of its monitoring programme is set out in the Code.[105]

Following the Benczkowski Memorandum, appropriate tailoring has become increasingly important and gives parties the opportunity to think carefully about the shape the monitorship should take, but it remains to be seen whether the DOJ under President Biden will continue to emphasise narrow tailoring.[106] In Walmart's June 2019 settlement with the DOJ over FCPA violations, the company agreed to a monitorship whose mandate was narrowed both by geography (to four countries and the company's headquarters) and subject matter (to specified Key Risk Areas).[107] The agreement specifically stated: 'The Monitor shall not conduct a comprehensive review of all business lines, all business activities, or all countries.'[108] Likewise, Ericsson and The Bank of Nova Scotia both entered into DPAs in the past two years – Ericsson over FCPA violations and The Bank of Nova Scotia over fraudulent trading practices – and each DPA limited the role of the monitor as such: '[T]he Monitor is *not expected* to conduct a comprehensive review of all business lines, all business activities, or all markets.'[109]

The monitor is an independent third party and does not serve as an employee or agent of either the corporation or the government.[110] Likewise, the monitor does not have an attorney–client relationship with either the corpora-

104 Critics complain that '[l]ittle is publicly disclosed about what specifically they are supposed to accomplish [and] what they discover in their examinations'. Ensign and Colchester, supra note 99.

105 See, in particular, DPA Code of Practice, para. 7.21.

106 See supra notes 55 and 56 and accompanying text.

107 Dep't of Justice Non-Prosecution Agreement with Walmart, Inc., Attachment C at ¶ 2, 20 June 2019, available at https://www.justice.gov/opa/press-release/file/1175791/download. The monitor's mandate was limited to an assessment of the 'Key Risk Areas', defined as 'anti-corruption-related internal auditing controls related to anti-corruption, record-keeping, and financial reporting policies and procedures of the Company as they relate to permits and licensing, real estate development and construction . . . donations . . . and third-party intermediaries', with several explicit carve-outs. The monitor's mandate was further limited to four countries, as well as Walmart's headquarters in Arkansas. Id.

108 Id. at ¶ 8.

109 Dep't of Justice Deferred Prosecution Agreement with Ericsson, Attachment D at ¶ 8, 6 December 2019, available at https://www.justice.gov/opa/press-release/file/1272151/download; Dep't of Justice Deferred Prosecution Agreement with Bank of Nova Scotia, Attachment D at ¶ 8, 19 August 2020, available at https://www.justice.gov/opa/press-release/file/1306141/download (emphasis added).

110 Notably, some corporations have taken to hiring their own internal monitors following the government's implementation of a monitor. For example, as part of Western Union's 2010 settlement, Western Union received a monitor. Independently, Western Union also hired a consultant, leading to what in effect was a 'dual system of internal monitors – one

© Law Business Research 2021

tion or the government. Nonetheless, it is critical for the monitor to have an open dialogue with, and co-operation from, the corporation and the government throughout the duration of the monitorship, which may include 'iterative work plans, planning meetings prior to any substantive work, and mid-review meetings'.[111] The parties should also stipulate what, if any, role the government or court should play in resolving disputes that may arise between the monitor and the corporation.[112]

Though the monitor does not take on a prosecutorial function, he or she may nonetheless uncover continuing or undisclosed misconduct. The monitorship agreement 'should clearly identify any types of previously undisclosed or new misconduct that the monitor will be required to report directly to the [government]'. And, on the other hand, the agreement should identify any misconduct that the monitor can, in its discretion, report to the government, the corporation or both.[113]

Duration of the monitorship 33.5.2

Monitorships can range from months to several years. The duration of the monitorship will in large part depend on the scope of the monitorship, and in particular the extent of the problems found and the necessary remedial measures.[114] When negotiating duration, the parties should be mindful of, *inter alia*, the 'nature and seriousness of the underlying misconduct', the 'pervasiveness and duration of the misconduct', the complicity of senior management, the 'corporation's history of similar misconduct', the corporate culture, the 'scale and complexity of any remedial measures contemplated by the agreement, including the size of the entity or business unit at issue', and the current 'stage of design and implementation of remedial measures'.[115]

Another issue to consider is the terms under which the monitorship may be extended. Some monitorship agreements, particularly those that are supervised by the courts, provide for extensions where certain milestones have not yet

stipulated by the settlement and the other hired by the money-transfer firm'. Ensign and Colchester, supra note 99.

111 F Joseph Warin, Michael S Diamant and Veronica S Root, 'Somebody's Watching Me: FCPA Monitorships and How They Can Work Better', 13 *U. Pa. J. Bus. L.* 321, 364 (2011), available at http://scholarship.law.upenn.edu/jbl/vol13/iss2/1.

112 Grindler Memorandum, supra note 13, § II.

113 Morford Memorandum, supra note 11, at 7. Critically, undisclosed or continuing misconduct may invalidate the terms of the settlement and lead to an extension of the term and scope of the monitorship.

114 Id., at 7–8.

115 Id. at 7. See Benczkowski Keynote Address at the Ethics and Compliance Initiative 2019 Annual Impact Conference, supra note 62 (noting that a monitorship limited to two years was appropriate as part of Fresenius Medical Care's FCPA settlement, because the company 'had made a number of improvements to its compliance program but had not yet fully tested that program').

© Law Business Research 2021

been met. Where judging the achievement of those milestones is within the monitor's purview, the monitor may have an incentive to declare the milestones incomplete so that the term may be extended. In other cases, the monitorship agreement will permit the government to extend the monitorship at its discretion if the corporation has not satisfied its obligations under the settlement, and provide for early termination if the corporation can demonstrate 'a change in circumstances sufficient to eliminate the need for a monitor'.[116] For example, in 2016 Odebrecht entered into a plea agreement with the DOJ to resolve FCPA violations, which included the largest corruption fine ever at that time.[117] Part of the plea deal required Odebrecht to retain a monitor for three years and to adopt and implement an effective compliance and ethics programme.[118] The agreement scheduled the monitorship to expire on 20 February 2020; however, the DOJ determined that Odebrecht failed to fulfil its terms.[119] First, Odebrecht failed to adopt and implement the monitor's recommendations and to allow the monitor to complete the monitorship.[120] Second, Odebrecht failed to implement and maintain a compliance and ethics programme.[121] As a result, the DOJ extended the monitorship to 16 November 2020 – an additional 270 days.[122] In the United Kingdom, this ability to extend monitorships

116 Morford Memorandum, supra note 11, at 8 ('For example, if a corporation ceased operations in the area that was the subject of the agreement, a monitor may no longer be necessary. Similarly, if a corporation is purchased by or merges with another entity that has an effective ethics and compliance program, it may be prudent to terminate a monitorship.').

117 Letter advising the Court of the parties' agreement to extend the term of the plea agreement, *United States v. Odebrecht S.A.*, No. 16-cr-643 (RJD) (E.D.N.Y. 29 Jan. 2020), ECF 170; Clara Hudson, 'Odebrecht failed to fulfil monitorship obligations, DOJ says', Global Investigations Review (3 February 2020), https://globalinvestigationsreview.com/article/jac/1213971/odebrecht-%E2%80%9Cfailed-to-fulfil%E2%80%9D-monitorship-obligations-doj-says.

118 Letter advising the Court of the parties' agreement to extend the term of the plea agreement, *Odebrecht S.A.*, No. 16-cr-643 (RJD).

119 Id.

120 Id.

121 Id.

122 Id. Similarly, after Credit Suisse admitted to aiding US tax evasion, the New York State Department of Financial Services appointed a monitor for what was anticipated to be a two-year monitorship. However, shortly after the monitorship began in October 2014, a tolling period was triggered because Credit Suisse could not produce information at the pace and volume required by the monitor. After more than three years of monitorship, the Department of Financial Services entered a consent order requiring Credit Suisse to engage an independent consultant for an additional year. John Letzing, 'Credit Suisse's Tardiness Likely to Extend Monitor's Sojourn', *Wall Street J.* (6 Jan. 2016), www.wsj.com/articles/credit-suisses-tardiness-likely-to-extend-monitors-sojourn-1452084986; N.Y. Dep't of Fin. Services Consent Order, *In the Matter of Credit Suisse AG* (13 Nov. 2017), available at https://www.dfs.ny.gov/system/files/documents/2020/03/ea171113_credit_suisse.pdf.

© Law Business Research 2021

has been formally recognised in the Code, subject to the extended term of the monitorship not exceeding the length of the DPA itself.[123]

Hybrid monitorships – in which the monitor serves for approximately 18 months and the corporation self-reports for the following 18 months – are also becoming increasingly common, especially in the context of FCPA investigations.[124] As a further nuance, the DOJ has, in some instances, agreed to defer to a pre-existing monitorship in lieu of establishing its own monitorship. As one example, the December 2015 settlement between Alstom and the DOJ, for various FCPA violations, required that Alstom be subject to an independent monitor. However, Alstom was already subject to a monitor in connection with a 2012 settlement with the World Bank. Rather than implement a second monitor, the DOJ agreed to defer to the existing World Bank-appointed monitor, provided that, *inter alia*, Alstom self-report to the DOJ 'at no less than twelve-month intervals during a three-year term'.[125]

Rolls-Royce reached a similar resolution in its January 2017 settlement with US, UK and Brazilian authorities over bribery and corruption charges (and, in the United States, FCPA charges). At the time, Rolls-Royce already had an independent monitor – Lord Gold – who was appointed to review the company's anti-bribery and corruption compliance in connection with a 2013 settlement with the SFO. Though the company's 2017 DPA with the SFO did not impose a second monitor, it did require Rolls-Royce, *inter alia*, to procure a further report from Lord Gold outlining recommendations for change and produce a written plan of how it would implement these recommendations.[126] Likewise, the company's DPA with the DOJ did not implement a further monitor, but did require the company to report to the DOJ at least once a year for the next three years and to produce a series of reports.[127] When the SFO applied to the English Court for approval of the DPA, the senior

123 See DPA Code of Practice, para. 7.19.

124 FCPA Digest, 'Recent Trends and Patterns in the Enforcement of the Foreign Corrupt Practices Act' at 2, 6, Shearman & Sterling (6 Jan. 2014), available at www.shearman.com/~/media/Files/Services/FCPA/2014/FCPADigestTPFCPA010614.pdf. For example, the DOJ's DPA with Panasonic required a two-year monitorship, after which Panasonic was required to undertake follow-up reviews for the remainder of the agreement. Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp. at 12–13, 30 April 2018, available at https://www.justice.gov/opa/press-release/file/1058466/download.

125 Dylan Tokar, 'With Alstom Monitor Agreement, DOJ Tries Something New', Global Investigations Review (4 Feb. 2015), available at http://globalinvestigationsreview.com/article/1023537/with-alstom -monitor-agreement-doj-tries-something-new.

126 Deferred Prosecution Agreement between the SFO and Rolls-Royce, paras. 25–34, available at http://iaicm.org/wp-content/uploads/formidable/9/Rolls-Royce-SFO-DPA-17Jan2017.pdf.

127 Deferred Prosecution Agreement at 4–5, D-1, *United States v. Rolls-Royce plc*, No. 16-0247 (S) (S.D. Ohio, 20 Dec. 2016) ('Based on the Company's remediation and the state of its compliance program, and the Company's agreement to report to the Fraud Section and the Office as set forth in Attachment D to this Agreement, the Fraud Section and the Office determined that an independent compliance monitor was unnecessary[.]').

© Law Business Research 2021

judge who heard that application, Sir Brian Leveson, President of the Queen's Bench Division, expressly referred to the appointment of Lord Gold and the ongoing monitoring process as important factors indicating that Rolls-Royce had properly addressed issues of corporate compliance; this made the DPA (as opposed to criminal prosecution) an appropriate outcome.[128]

The 2019 *Serco Geografix* DPA took into consideration the fact that the parent company, Serco Group, had adopted an ongoing corporate renewal programme in 2013, which had been approved by the UK government, to improve assurance mechanisms and working practices within all companies in the group. In the approved judgment, Justice Davis said that this amounted to a significant remedial measure.[129]

33.5.3 Creating a work plan

Under the ABA Standards, the monitor should draft a detailed work plan at the outset of the monitorship, with input from the corporation and the government.[130] This is also a requirement of the UK regime under the Code, which stipulates that a work plan should be prepared even before the monitor's appointment is finally approved.[131] The work plan will ordinarily include an overview of the monitor's role and objectives, a description of the corporation's policies and procedures to be evaluated, a list of documents the monitor seeks to review, and a list of persons the monitor seeks to interview. The work plan should also include a proposed timeline for reaching certain milestones, such as a review of documents concerning the corporation's compliance programme, interviews with senior management, the board of directors and audit committee, and periodic reports of the monitor's findings.[132] In the United Kingdom, the work plan is required to set out provisions for costs and even to state with what frequency the monitor intends to report to the prosecutor.[133]

Not only does a detailed work plan help control costs and increase transparency, but it also helps prepare all parties for the monitorship.[134] Accordingly, the corporation will have a better understanding of what can be expected, and the act of preparing the work plan helps the monitor become familiar with the company's culture and risk tolerance. Further, a detailed work plan helps ensure

128 *Serious Fraud Office v. Rolls-Royce plc* [2017] Lloyd's Rep FC 249 at paras. 43–47 and 61–64.

129 *Serious Fraud Office v. Serco Geografix Limited* [2019] Lloyd's Rep FC 518 at para. 25.

130 If disclosing the work plan to the company would limit the monitor's effectiveness, however, the parties should consider an alternative arrangement. See ABA Standards for Monitors, § 24-3.3(3).

131 See DPA Code of Practice, para. 7.18.

132 Jason T Wright, 'The Corporate Compliance Monitor's Role in Regulatory Settlement Agreements', Stout (1 Mar. 2014), https://www.stout.com/en/insights/article/corporate-compliance-monitors-role-regulatory-settlement-agreement.

133 See DPA Code of Practice, para. 7.18.

134 See Warin, supra note 111, at 360 (noting that the work plan also serves as a 'gloss on the settlement agreement to be applied in subsequent years of the monitorship').

© Law Business Research 2021

that the monitor's expectations for the corporation are reasonable and that the government is comfortable with the monitor's approach.[135]

Reviewing documents and interviewing witnesses 33.5.4

To serve as an effective monitor and issue tailored recommendations to the corporation, the monitor must understand the corporation and its business. To develop this understanding, the monitor must have wide access to the documents and information deemed reasonably necessary to carry out the monitorship.[136] A recurring problem, however, is that given the monitor's independence, corporations are hesitant to disclose sensitive information. Under the ABA Standards, the corporation is not required to provide documents covered by the attorney–client or work-product privilege, or documents for which disclosure would be 'inconsistent with applicable law'.[137] A similar approach is adopted under the UK Code, which requires the company to grant the monitor 'complete access to all relevant aspects of its business during the course of the monitoring period', but does not affect the company's right to assert legal professional privilege over relevant documents.[138]

See Chapters 36 and 37 on privilege

It may also be necessary for the monitor to interview personnel, from low-level employees to senior management. The monitorship agreement should ordinarily address issues of employee rights that could arise during the monitorship, including privacy rights and the right to counsel – issues that take on added complexity where the monitor's review is cross-border. Ordinarily, the monitor should inform interviewees of his or her identity and explain why information is being collected. The monitor should also inform interviewees whether they are the target of the monitor's investigation and of their right to have counsel present during the interview. Where an employee chooses to exercise the right to counsel, the monitor must respect that decision.[139]

See Chapters 5 and 6 on beginning an internal investigation; 7 and 8 on witness interviews; and 13 and 14 on employee rights

The monitor may find it advisable to inform interviewees of the degree to which the information being provided will remain confidential and what, if anything, the monitor is required to do with that information. In some

135 Wright, supra note 132.

136 See Ensign and Colchester, supra note 99 (noting that the monitorship involved more than 3,500 meetings with HSBC staffers, 11,500 document requests and over 2 million pages of documents).

137 ABA Standards for Monitors, § 24-4.2(1)(a)–(2)(a). Despite the monitor's independence, the monitor still has a duty to the corporation by nature of the appointment. Thus, the monitor cannot use proprietary or confidential information obtained during the monitorship for any purpose other than in furtherance of the monitorship. Where proprietary information is disclosed, the monitor and corporation should work together to ensure this information remains confidential. The parties should also stipulate how the monitor is to return any confidential or proprietary documents upon completion of the monitorship.

138 See DPA Code of Practice, s.7.14.

139 Except in limited circumstances, a company is not required to provide counsel or pay for counsel for employees being interviewed.

© Law Business Research 2021

circumstances, such as when information would otherwise be hard to extract, it may be appropriate for the monitor to have the authority to collect information confidentially to protect its sources.[140]

33.5.5 Issuing recommendations and reports

During the course of the monitorship, the corporation and monitor should work together to develop recommendations for improvement of the corporation's compliance programme and to prevent repeated corporate misconduct. The recommendations should be mindful of local laws concerning, for example, data privacy and privilege. Depending on the scope and duration of the monitorship, the monitor may summarise his or her findings and recommendations in periodic reports to the government or court, or issue a single report at the end of the monitorship.[141] As negative findings in the report have the potential to significantly harm the corporation, in some circumstances the monitor may provide the corporation with a preliminary draft and invite comments.[142] Ultimately, however, the report is issued by the monitor alone, and must reflect the monitor's honest conclusions and recommendations.

Where the corporation disagrees with one of the monitor's recommendations, the corporation may reject it within a reasonable time, provided the government is informed. The government may consider this rejection when evaluating whether the corporation has fulfilled its obligations under the settlement.[143] Under the Grindler Memorandum, where a corporation rejects a monitor's recommendation on the basis of cost, it should provide a written proposal of 'an alternative policy, procedure, or system designed to achieve the same objective or purpose'.[144]

In the United Kingdom, the confidentiality of a monitor's reports and correspondence is expressly recognised in the Code, and its disclosure is restricted to the company, the prosecuting authority and the court (except as otherwise permitted by law).[145] Similarly in the United States, the government routinely denies Freedom of Information Act requests filed by news outlets for the production of monitor reports.[146] However, the public's right of access to

140 ABA Standards for Monitors, § 24-4.2(4)(d).

141 Morford Memorandum, supra note 11, at 6.

142 ABA Standards for Monitors, § 24-4.3(1)(d). Giving the corporation the opportunity to review a draft report may improve the quality of the report, as the corporation can correct any errors and, where applicable, provide evidence to rebut the monitor's negative findings.

143 Morford Memorandum, supra note 11, at 6. For example, after Standard Charter settled charges that it disguised transactions that could have violated US sanctions, two monitors were appointed as well as one 'independent consultant'. The monitors' findings that inadequate controls were used led to an additional $300 million fine. Ensign and Colchester, supra note 99.

144 Grindler Memorandum, supra note 13, § II.

145 See DPA Code of Practice, para. 7.20.

146 Ensign and Colchester, supra note 99.

© Law Business Research 2021

such reports has been litigated in relation to the deferred prosecution agreement between the DOJ and HSBC.[147]

By way of background, in 2012, HSBC reached a US$1.9 billion settlement with the government and secured a five-year DPA for HSBC's failure to comply with anti-money laundering laws and US sanctions.[148] In an unusual turn of events, the court approved the DPA on the condition that the court could continue to exercise 'supervisory' control over the case.[149] A monitor was appointed as part of the settlement and issued a 1,000-page report in January 2015, a copy of which was filed under seal with the court. Thereafter, an HSBC mortgage customer asked the court to unseal the report so he could determine whether HSBC continued to engage in 'unsafe and unsound business practices'.[150] The lower court held that the report qualified as a 'judicial record' that should be filed publicly, and that 'the public has a First Amendment right to see the Report', though HSBC and the government could suggest redactions and parts to remain under seal.[151] HSBC and the government opposed the unsealing, claiming it 'could provide a "road map" for criminals seeking to launder money'.[152] HSBC's lawyer said the court's order also called into question assurances given to foreign regulators who had provided information to the monitor on condition the report be kept secret.[153] On 12 July 2017, the United States Court of Appeals for the Second Circuit reversed the lower court's decision noting that 'a district court's role vis-à-vis a DPA is limited to arraigning the defendant, granting a speedy trial waiver if the DPA does not

147 The HSBC matter represents the most public instance of a party seeking access to a monitor's report; however, it is not the only such example. See *In re Depuy Orthopaedics, Inc. Pinnacle Hip Implant Prod. Liab. Litig.*, No. 11 MD 2244, 2013 WL 2091715 (N.D. Tex. 15 May 2013) (ordering disclosure of monitor's report in a product liability matter).

148 In December 2017, the DOJ found that HSBC had successfully addressed the issues related to its case and sought to dismiss. Evan Weinberger, 'DOJ Seeks Dismissal of HSBC Money Laundering Case', *Law360* (12 Dec. 2017), https://www.law360.com/articles/993914/doj-seeks-dismissal-of-hsbc-money-laundering-case.

149 See Christie Smythe, 'Judge Lets Sun Shine on Secret HSBC Money Laundering Report', Bloomberg (29 Jan. 2016), www.bloomberg.com/news/articles/2016-01-29/judge-lets-sun-shine-on-secret-hsbc-report-on-money-laundering.

150 Nate Raymond, 'HSBC money laundering report's release likely delayed: U.S. judge', Reuters (10 Feb. 2016), www.reuters.com/article/us-hsbc-moneylaundering-idUSKCN0VI28H. See *United States v. HSBC Bank USA NA*, No. 12 CR 763 (JG), 2016 WL 347670, at *1, *6 (E.D.N.Y. 28 Jan. 2016), motion to certify appeal denied, No. 12-0763, 2016 WL 2593925 (E.D.N.Y. 4 May 2016) (inviting the parties to suggest further redactions to the report).

151 *HSBC Bank USA NA*, 2016 WL 34760, at *1, *6. ZTE's monitor reports may be particularly susceptible to this type of argument, given that the plea agreement as amended by Judge Kinkeade refers to the monitor as a 'judicial adjunct' and provides that all monitor reports be filed with the court, albeit under seal and subject to in-camera review. See supra notes 87–92 and accompanying text.

152 Raymond, supra note 150.

153 Id.

© Law Business Research 2021

represent an improper attempt to circumvent the speedy trial clock, and adjudicating motions or disputes as they arise'.[154] Given the limited supervisory role of courts in the DPA context, the Second Circuit held that a monitor's report is not a judicial record because it is not 'relevant to the performance of the judicial function'.[155] The holding, which relies upon and is consistent with the DC Circuit Court of Appeals' decision in *United States v. Fokker Services BV*, limits both a district court's initial judicial review of a DPA and its subsequent oversight of the DPA's execution.[156]

The District Court for the District of Columbia made a similar ruling in *100Reporters LLC v. United States Department of Justice*, concerning monitor reports issued in the wake of Siemens' 2008 settlement with the United States and Germany. There, reporters sued to obtain the reports under the Freedom of Information Act (FOIA). In a March 2017 decision, the court acknowledged that significant portions of the report may be exempt from production under FOIA – for example, because they contain 'classic attorney work-product' and 'information [that] cuts to the core of Siemens' business', on which a competitor could rely to Siemens' detriment – but the court was not prepared to find that all information should be so shielded.[157]

Given the remaining uncertainty over the confidentiality of the monitor's report, it has become best practice – as confirmed by ABA Standard 24-4.3(4) – for the government and the corporation to determine whether reports will be made public when negotiating the settlement agreement:

> *To perform its duties, the monitor needs access to unprivileged, confidential and proprietary business information of the corporation and communications among the corporation, the monitor and the government need to be candid and complete over an extended period.*
>
> *Recognising that corporate information included in monitor reports may be used unfairly by competitors and others to disadvantage the corporation, DPAs and NPAs typically reflect the parties' intentions to maintain the confidentiality of monitor reports.*[158]

Where a proposed settlement agreement instituting a monitorship lacks such explicit proviso for confidentiality, counsel should seek to revise and include it.

---

154 *United States v. HSBC Bank USA, N.A.*, 863 F.3d 125, 129 (2d Cir. 2017).

155 Id. at 137.

156 See *United States v. Fokker Services B.V.*, 818 F.3d 733 (D.D.C. 2016).

157 *100Reporters LLC v. U.S. Dep't of Justice*, No. 14-1264-RC, at 3, 32, 58 (D.D.C. 31 Mar. 2017) (finding that the DOJ had justified withholding portions of the report under certain exemptions to FOIA, but had not justified the withholding of all portions of the report or demonstrated that the report could not be segregated for purposes of partial production).

158 Karen F Green and Timothy D Saunders, 'Minding the Monitor: Disclosure of Corporate Monitor Reports to Third Parties', Bloomberg BNA (25 Mar. 2014).

© Law Business Research 2021

Costs and other considerations 33.6

Monitorships can be extremely expensive, with monitors collecting multimillion-dollar fees, to be paid for by the corporation (and ultimately its shareholders).[159] For example, Ericsson recently disclosed that it had set aside US$58 million to cover the costs of its impending monitorship.[160] Critics note that the rise in monitorships has created 'a lucrative cottage industry made up of former prosecutors and small consulting firms', some of which even offer expertise in assisting corporations monitor their monitors.[161] Others argue that the cost of the monitorship will be offset against the fines levied on the corporation and that the imposition of a monitor may help sway the government in favour of reduced fines.[162]

The ultimate cost of the monitorship will largely depend on the scope and duration of the monitorship. Cost will also be influenced by the complexity of the settlement agreement, the state of the corporation's existing compliance programme, and the geographic markets and industries in which the corporation operates. The monitor should take these various factors into consideration when providing the corporation with a projected budget. The monitor and the corporation should also consider and agree on an hourly rate or a fixed rate, any applicable rate adjustments and a potential fee cap. Further, to increase transparency and mitigate the risk of conflicts, the monitor should provide regular updates on the costs being incurred and expected to be incurred.[163]

As one example of the issues that can arise because of costs, in 2014, Apple moved to disqualify its antitrust monitor for what it viewed as excessive billing and unprofessional conduct where the monitor, *inter alia*, had charged a rate of

159 Both the Morford Memorandum and the Grindler Memorandum counsel the need for prosecutors to be mindful of the costs of monitors and their potential impact on the corporation when negotiating settlements. Grindler Memorandum, supra note 13, § II (noting that the government 'should help to instill public confidence in the Department's use of monitors, including the Department's mindfulness of the costs of a monitor and their impact on a corporation's operations'); Morford Memorandum, supra note 11, at 2 (noting that prosecutors must be mindful of 'the cost of a monitor and impact on the operations of a corporation').

160 Adam Dobrik, 'DOJ picks Ericsson monitor', Global Investigations Review (11 May 2020), https://globalinvestigationsreview.com/article/jac/1226647/doj-picks-ericsson-monitor.

161 Rachel Louise Ensign, 'Judge Rules HSBC's Outside Monitor's Secret Report Should be Made Public', *The Wall Street J.* (29 Jan. 2016), www.wsj.com/articles/judge-rules-hsbcs-outside-monitors-secret-report-should-be-made-public-1454086003; see also Ensign and Colchester, supra note 99.

162 Whereas fines are usually due in one lump sum, payments for monitors are commonly billed monthly. See Wright, supra note 132 ('More often than not, however, this cost is far less than what the company would otherwise pay in fines, possible debarment, or legal fees in defending an enforcement action through trial.'); Patricia M Sulzbach, 'Independent Corporate Monitors: A Company's Friend or Foe?', ABA White Collar Crime Comm. Newsletter (18 Apr. 2013).

163 See also ABA Standards for Monitors, § 24-3.4.

© Law Business Research 2021

US$1,000 per hour in fees.[164] The motion was denied by the Southern District of New York in an order affirmed by the Second Circuit, but the Second Circuit noted that the issues raised had 'considerable resonance because the fairness and integrity of the courts can be compromised by inadequate constraint on a monitor's aggressive use of judicial power'.[165] The monetary cost of corporate monitorships to the affected business was one of the two guiding principles that Trump-era Assistant Attorney General Brian Benczkowski noted should determine the imposition of such a monitorship in his 2018 memorandum.

33.7 Conclusion

Since their first applications during the 1990s, the use of monitors has rapidly expanded across industries and offences: banks, energy companies, unions, car manufacturers and fire departments have all been (or currently are) subject to oversight by monitors. Implemented to address a myriad of wrongs ranging from fraud and racketeering to discriminatory hiring practices, monitorships were in many ways viewed as panaceas.

Rising costs and increasing concerns about their efficacy have resulted in far greater scrutiny of all proposed monitorships. Where the past two decades represent an expansion in the breadth of cases where monitors were contemplated, the next two are likely to focus on and refine that scope. The ongoing debates over whether monitors' reports should be public, the degree to which monitors are truly independent, and how monitors should be selected will result not only in additional litigation, but will force an evolution in how monitorships are used as settlement tools. The issues identified throughout this chapter are live controversies, each likely to distil and develop the body of case law governing monitorships, ultimately resulting in a body of jurisprudence that imposes default standards of disclosure, transparency, control and authority on monitors, the government and defendants alike.

164 *United States v. Apple, Inc.*, 992 F. Supp. 2d 263 (S.D.N.Y. 2014).

165 *United States v. Apple, Inc.*, 787 F.3d 131, 133–34 (2d Cir. 2015).

© Law Business Research 2021

34

Parallel Civil Litigation: The UK Perspective

Nichola Peters and Michelle de Kluyver[1]

Introduction 34.1

The conduct under review in investigations can generate a range of parallel proceedings. These can precede the investigation, follow on from the investigation findings or, frequently, arise in the course of an investigation. It can be a particular challenge to manage parallel proceedings, which engage their own procedural rules and can force the pace of investigations or create other tensions with the investigative process. This chapter deals with the types of issues and parallel proceedings most likely to arise in complex investigations.

Stay of proceedings 34.2

Where a company subject to investigation is also involved in ongoing civil proceedings (before the courts or an arbitral tribunal) that relate to the conduct under investigation, the parties may seek to stay those proceedings pending the outcome of the investigation. This would often be an ideal solution to managing the tensions they introduce but obtaining a stay can be difficult and is not automatic.

Civil litigation 34.2.1

There are many reasons why a court may stay proceedings. For instance, to allow for arbitration, for the dispute to be tried by national courts of another jurisdiction or for other case management purposes (for example, to permit

1 Nichola Peters and Michelle de Kluyver are partners at Addleshaw Goddard LLP. Michelle de Kluyver co-authored this chapter for the first edition with Edward McCullagh and would like to thank him for his contribution as co-author and then as author of later editions, as well as Jonathan Hitchin of Allen & Overy LLP for his support on all earlier editions.

© Law Business Research 2021

commercial settlement negotiations, or to allow a ruling on a relevant issue to be delivered in a separate case). The court may do so on various legal bases. As well as possessing inherent jurisdiction to manage proceedings,[2] the court is empowered under the Civil Procedure Rules (CPR) to stay proceedings in part or in whole, either indefinitely or until a specified date or event.[3] The court may stay proceedings in specific circumstances pursuant to certain other statutes.[4]

In circumstances where there are related criminal proceedings, the following principles (among others) will apply to the exercise of the court's discretion to stay civil proceedings:[5]

- the court will only consider staying the civil proceedings if there is a real risk of serious prejudice that may lead to injustice;[6]
- the court will exercise its discretion by reference to the competing considerations between the parties – the court has to balance justice between the parties;[7]
- the fact that a defendant, by serving a defence in civil proceedings, would be giving advance notice of their defence in criminal proceedings, carries little weight in the context of an application for a stay of civil proceedings;
- it is not enough that both the civil and criminal proceedings arise from the same facts, or that the defence of the civil proceedings may involve a defendant taking procedural steps (such as exchanging witness statements, and providing disclosure of documents) that might not be imposed on them in the criminal proceedings;[8] and
- even if the court is satisfied that there is a real risk of serious prejudice leading to injustice if the civil proceedings continue, the proceedings should nevertheless not be stayed if safeguards can be imposed in respect of the civil proceedings that provide sufficient protection against the risk of injustice.

A stay of proceedings puts a stop to their further conduct at the stage they have reached, apart from the taking of any steps allowed by the CPR or the terms of the stay. The court may also impose a stay on the effects of an action, such as a stay of execution of orders of a lower court pending appeal. Proceedings can be continued if the stay is lifted.

2 See, e.g., *China Export & Credit Insurance Corporation v. Emerald Energy Resources Limited* [2018] EWHC 1503 (Comm), [61].

3 CPR, Part 3.1(2)(f).

4 For example, Arbitration Act 1996, s.9.

5 See *Akcine Bendrove Bankas Snoras (in bankruptcy) v. Antonov* [2013] EWHC 131 (Comm), [18].

6 *R v. Panel on Takeovers and Mergers, ex parte Fayed* [1992] BCC 524, 531.

7 *Panton and others v. Financial Institutions Services Ltd* [2003] UKPC 95, [11].

8 *FSA v. Anderson* [2010] EWHC 308 (Ch), [19].

© Law Business Research 2021

Arbitral proceedings 34.2.2

In England, as in many other jurisdictions, procedural matters in arbitration are governed first and foremost by parties' agreement. Aspects of applicable arbitral procedure may be set out expressly in an arbitration agreement, be contained in the parties' chosen institutional arbitration rules (whether such choice is expressed in the arbitration agreement or otherwise) or subsequently be agreed by the parties to a dispute, whether on an *ad hoc* basis or, for instance, in the tribunal's agreed terms of appointment. Where parties do not reach agreement, procedural arrangements are otherwise within the discretion of the arbitral tribunal as a matter of English law, subject to the tribunal's general duties to act fairly and impartially as between the parties and to adopt procedures suitable to the circumstances of the particular case.[9]

An arbitral tribunal may, in exercise of its discretion, elect to stay the arbitral proceedings for a variety of reasons. For instance, at the request of one or both of the parties pending settlement negotiations, upon a party failing to comply with an order to provide security for costs or pending the determination of a preliminary point of law by a court.[10] A tribunal might also stay proceedings to avoid the risk of inconsistent decisions where parallel judicial or regulatory proceedings are ongoing, particularly where such proceedings are ongoing in the same jurisdiction as the arbitral seat. In all cases, a tribunal's decision will depend on the propriety of ordering a stay in all the relevant circumstances, which may, in the regulatory context, depend on the identity of the regulator and the extent to which the outcome of the regulatory investigation is likely to impact the matters at stake in the arbitration itself.

Multi-party litigation 34.3

Under English law, class actions do not feature as part of the parallel litigation landscape to the extent that they do in the United States (in particular, securities litigation). Nonetheless, companies may face civil actions brought by multiple parties in a variety of ways and we describe them for completeness. The two main procedural mechanisms for multi-party litigation envisaged by the CPR are representative actions and group litigation orders.[11] Additionally, a form of collective proceeding exists in the competition law context, although this type of action is still in its infancy in the United Kingdom.

Representative actions 34.3.1

Representative actions allow persons, in certain circumstances, to represent others in legal proceedings (the represented persons are not joined to the

9 Arbitration Act 1996, ss.33 and 34.

10 ibid., s.45.

11 See further *Zuckerman on Civil Procedure: Principles of Practice*, Adrian Zuckerman (4th edn, Sweet and Maxwell, 2021); *Improving Access to Justice through Collective Actions* (Civil Justice Council, 2008).

© Law Business Research 2021

action as parties). The CPR provide that such actions may be brought where more than one person has the same interest in a claim.[12] Judgments or orders given in representative actions are normally binding on all persons represented in the claim, but may only be enforced by or against non-parties with the court's permission.[13]

Representative actions are not extensively used. The provisions of the CPR relating to such actions are restrictive; in particular, the 'same interest' requirement. A further potential deterrent is that represented persons are not liable for the costs of representative actions. Instead, costs are assessed under CPR Part 44 and paid by the representing party, although the court does have jurisdiction to order that costs be paid by a non-party in exceptional circumstances.

34.3.2 Group litigation orders

Where claims give rise to common or related issues of fact or law, the court may make a group litigation order (GLO), which provides for the case management of claims covered by the order.

The GLO will contain directions about the establishment of a group register on which the claims to be managed under the GLO will be entered, and will specify the court that will manage the claims on the register.[14] The GLO procedure is 'opt-in' in nature. Claims must be issued before they can be entered on a group register, and an application for details of a case to be entered on a group register may be made by any party to the case. The management court may set a cut-off date after which no further claims may be added to the group register without the court's permission.

The GLO will also specify the 'GLO issues', which will identify the claims to be managed as a group under the GLO.[15] Judgments or orders given or made in a claim on the group register in relation to the GLO issues are binding on the parties to all other claims on the group register.[16] The court may direct that certain claims on the group register should proceed as test cases.

GLOs have been utilised in a range of different types of dispute, but are not particularly widely used and have been subject to criticism.

34.3.3 Joint claims

Multiple parties can also be joined to the same claim. The CPR give the court a range of powers to add or substitute parties to proceedings.[17] Any number of

12 Representative actions may also be brought in more limited circumstances pursuant to the Civil Procedure Rules (CPR), Part 19.7.

13 CPR, Part 19.8A.

14 ibid., Part 19.11(2).

15 ibid.

16 ibid., Part 19.12(1).

17 ibid., Parts 19.1 and 7.3.

© Law Business Research 2021

claimants or defendants may be joined as parties to a claim,[18] and any number of claims may be covered by one claim form (provided those claims can be conveniently disposed of in the same proceedings). However, if a large number of parties are joined, this can lead to practical difficulties.

Test cases 34.3.4

There is no formal and generally applicable test case procedure before the English courts. However, when faced with large numbers of claims that raise common issues, the courts may use their case management powers to allow certain representative claims (usually selected by the parties) to proceed to determination and stay the remainder. While decisions in test cases have value as precedent, they are not determinative of other cases that raise common issues.

Test case procedures have, however, been introduced in certain specific contexts, for example:

- In appropriate circumstances, claims subject to a GLO may proceed as test cases.
- A Financial Markets Test Scheme (Test Scheme) has been introduced as part of the Financial List following a pilot scheme that was in effect from October 2015 to 30 September 2020.[19] The Test Scheme enables certain claims started in the Financial List to be determined as test cases, without the need for a present cause of action between the parties to the proceedings. The claims must raise issues of general importance in relation to which immediately relevant authoritative English law guidance is needed. Most recently, this included the topic of non-damage coverage under business interruption insurance policies in connection with the covid-19 pandemic.[20]

Financial Ombudsman or Business Banking Resolution Services 34.3.5

Complaints can be brought against financial services firms via an informal process of complaining to the firm and then to the Financial Ombudsman Service (FOS). The FOS applies a general 'fair and reasonable' test rather than applying strict law or regulation. The upper limit for an award from the FOS is now £350,000, and complaints can be brought to it by consumers, micro-enterprises and small businesses. Firms must comply with a detailed set of rules in the FCA Handbook on how they respond to complaints, and the FCA has investigated and issued several public fines against firms for poor complaints-handling. Equally, complaints to the FOS can prompt the FCA to

18 For instance, 255 claimants were joined to proceedings in the case of *Bravo and Others v. Amerisur Resources plc* [2020] EWHC 203 (QB).

19 CPR, Practice Direction 63AA.

20 *The Financial Conduct Authority v. MS Amlin Underwriting Limited and Others* [2020] EWHC 2448 (Comm) (Test Case). The decision was appealed to the Supreme Court, which handed down judgment on 15 January 2021: *The Financial Conduct Authority v. MS Amlin Underwriting Limited and Others* [2021] UKSC 1.

© Law Business Research 2021

investigate a particular product or service, and so there is an inherent interaction between financial services investigation and the FOS jurisdiction. Seven large banks have also recently devised the Business Banking Resolution Service, a voluntary scheme for resolving complaints of larger business customers.

34.3.6 Competition law claims

There are specialised collective proceedings for competition law claims.

Such proceedings may be brought before the Competition Appeal Tribunal (CAT) on a stand-alone basis (in which case, a complainant must prove an infringement of certain competition law rules) or on a follow-on basis (which requires an existing infringement decision establishing liability). Follow-on claims can be based on a competition infringement decision of the Competition and Markets Authority (CMA), or the CAT on an appeal from a decision of the CMA. European Commission infringement decisions can still form the basis of such claims provided the decision was made or the Commission's investigation was initiated before the end of the Brexit transition period (on 31 December 2020).

Claims will only be eligible for inclusion in collective proceedings if the CAT considers that they raise the same, similar or related issues of fact and law, and are suitable to be brought in collective proceedings.

Collective proceedings must be commenced by a person who proposes to be the representative in those proceedings, but they can only be continued if the CAT certifies them by making a collective proceedings order (CPO). The CAT may only make such an order if (1) it considers that it is just and reasonable for that person to act as a representative in the proceedings and (2) the claims are eligible for inclusion in collective proceedings.

The collective proceedings may be:

- 'opt-in' (brought on behalf of those class members who opt in); or
- 'opt-out' (brought on behalf of all class members, except for those who (1) opt out or (2) are not domiciled in the United Kingdom at a specified time, and do not opt in).

Class members can opt in or opt out by notifying the representative.

Judgments or orders of the CAT in collective proceedings are binding on all represented persons, except as otherwise specified. The CAT may not award exemplary damages in collective proceedings, and damages-based fee agreements for legal representatives are unenforceable if they relate to such proceedings.

The CAT granted its first CPO in 2021[21] authorising Walter Merricks as the class representative for an opt-out collective claim against Mastercard, on

21 *Walter Hugh Merricks CBE v. Mastercard Incorporated and Others* [2021] CAT 28. This was only the second opt-out collective claim to be brought in the CAT. The first such claim (*Pride Mobility Scooters*) was adjourned and then withdrawn in 2017 after a failed application

© Law Business Research 2021

behalf of a class comprising some 46.2 million individuals. The proceedings were commenced as a follow-on claim based on the European Commission's 2007 *Mastercard* decision.[22] The CAT had refused a CPO in 2017, on the basis that the claims were not suitable for an aggregate award of damages (broadly estimated at £14 billion) and that the proposals for distribution of any aggregate award did not offer a plausible way for approximating the loss suffered by individual claimants. The CAT's subsequent decision to grant a CPO followed a landmark judgment by the Supreme Court in December 2020[23] upholding an earlier Court of Appeal decision[24] finding that the CAT had set the threshold for certification too high with its requirements regarding suitability for aggregate damages and a method for distributing aggregate damages that would reflect the individual losses of members of the class. The Supreme Court ruling on certification and the CAT's eventual CPO in the *Mastercard* case pave the way for other pending CPO applications to proceed.[25]

As regards costs, the general rule in proceedings before the English courts is that the unsuccessful party will be ordered to pay the costs of the successful party. The CAT, however, has a broader discretion (at any stage of the proceedings) to make any order it thinks fit in relation to the payment of costs, and it may take account of (among other things) the conduct of all parties in relation to the proceedings. Costs will not normally be awarded against represented persons who are not the class representative, except in certain particular circumstances.

Settlement of opt-out (but not opt-in) collective proceedings is regulated by statute and overseen by the CAT (which must approve the terms of any settlement reached). In certain circumstances, collective settlements can also be reached in respect of claims even if a collective proceedings order has not been issued.

Collective redress schemes 34.3.7

The Financial Services and Markets Act (FSMA) is the main statutory framework for financial services regulation in England and Wales and contains the

for a CPO; the CAT did not dismiss the application for a CPO outright, but adjourned the proceedings to allow the representative an opportunity to reformulate the proposed subclasses of claimants and the methodology for calculating damages (*Dorothy Gibson v. Pride Mobility Products Ltd* [2017] CAT 9.

22 *Case C- 382/12 Mastercard and others v. Commission*, finding that Mastercard's multilateral interchange fees for certain cross-border payment card transactions infringed EU competition law.

23 *Walter Merricks CBE v. Mastercard Incorporated & Ors* [2020] UKSC 51.

24 *Walter Hugh Merricks CBE v. MasterCard Incorporated and Others* [2019] EWCA Civ 674.

25 For example, collective proceedings have been brought in relation to the European Commission's 19 July 2016 decision in Case AT.39824 – *Trucks*, concerning a cartel in the truck manufacturing industry. *UK Trucks Claim Limited v. Fiat Chrysler Automobiles N.V. and Others* was listed for December 2019, but the main hearing on the CPO applications was vacated pending the Supreme Court appeal in the *Mastercard* case.

© Law Business Research 2021

powers of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA). The FCA may (under section 404 and sections 404A to 404G of FSMA require firms authorised by the FCA (including payment service providers and electronic money issuers) to establish and operate a consumer redress scheme, where there is found to have been a widespread or regular failure by such a firm to comply with relevant requirements. The relevant requirements include both FCA rules and the general law, but do not extend to the FCA's Principles for Businesses. The power can be used if it appears to the FCA that, as a result of the failure, consumers have suffered (or may suffer) loss or damage in respect of which a remedy or relief would be available in legal proceedings, and the FCA considers that it is desirable to make rules to secure redress for consumers in respect of the failure. In addition, pursuant to section 404F(7) of FSMA, the FCA may vary the permission or authorisation of a firm to require it to establish and operate a scheme that corresponds to, or is similar to, a consumer redress scheme. The FCA also has administrative powers to require restitution under section 384 of FSMA, which it has previously used, for example, to establish a compensatory scheme for investors who suffered loss in connection with an overstatement of expected profits by Tesco plc in 2014.[26]

The FCA has used its power under section 404 of FSMA to introduce rules on consumer redress schemes in the CONRED section of its handbook. In practice, a great many more redress programmes, past business reviews and remediation programmes are conducted by firms under informal supervision of the FCA or a skilled person appointed by the FCA under section 166 FSMA without use of section 404 of FSMA or CONRED.

Statutory voluntary redress schemes have also been introduced in the competition law context, under which compensation may be offered by businesses as a result of infringement decisions made in respect of them. Such schemes are subject to the approval of the CMA.

34.4 Derivative claims and unfair prejudice petitions

34.4.1 Derivative claims

Members of a company can bring a derivative claim (pursuant to Part 11, Chapter 1 of the Companies Act 2006 (CA 2006)) in respect of a cause of action vested in the company, and seeking relief on its behalf. Such claims may only be brought in respect of a cause of action arising from an actual or proposed act or omission involving negligence, default, breach of duty or breach of trust by a director of the company, and the cause of action may be against the director or another person (or both).[27] Further guidance on permissible types of derivative actions was provided in the recent *Kallakis* case.[28]

26 FCA Final Notice to Tesco plc and Tesco Stores Limited dated 28 March 2017.

27 CA 2006, s.260(3).

28 *Kallakis v. AIB Group plc and Others* [2020] EWHC 460 (Comm).

© Law Business Research 2021

A member who brings such a derivative claim must apply for permission to continue it, and the CPR envisage a two-stage procedure for dealing with applications for permission to continue derivative claims (the company, and any other appropriate parties, are made respondents to the permission application at the second stage).

The court must take into account a number of particular factors when considering whether to grant permission, including the importance that a person acting in accordance with section 172 of the CA 2006 (duty to promote the success of the company) would attach to continuing the claim, and any evidence as to the views of members of the company who have no personal interest (direct or indirect) in the matter. However, permission must be refused in certain circumstances (for example, if the act or omission giving rise to the cause of action has been authorised or ratified).

Part 11 of the CA 2006 also includes a mechanism for members to apply (in appropriate circumstances) for permission (1) to continue as derivative claims certain claims brought by the company or (2) to continue derivative claims brought by other members of the company.

Unfair prejudice petitions 34.4.2

A member of a company may also apply to the court for an order under Part 30 of CA 2006 on the grounds that the company's affairs are being or have been conducted in a manner that is unfairly prejudicial to the interests of members generally, or of some part of its members (including at least the applicant), or that an actual or proposed act or omission of the company (including an act or omission on its behalf) is or would be so prejudicial.

The courts take a wide view of prejudice suffered by a shareholder, which need not be financial. The courts also have a very wide discretion in respect of what constitutes unfairness, although they do 'not sit under a palm tree'.[29] Typically, a member will not be entitled to complain of unfairness unless there has been some breach of the terms on which the member agreed that the company's affairs should be conducted, although there will be cases in which equitable considerations will make it unfair for those conducting the company's affairs to rely on their strict legal powers.

The court has a wide discretion to make such order as it thinks fit for giving relief in respect of the matters complained of in an unfair prejudice petition.[30] The most common order in practice is for the shares of the petitioner to be bought by the respondent at a price to be fixed by the court.

As unfair prejudice petitions generally raise numerous factual issues entailing examination of events over a considerable period of time, a high degree of case

29 *In re J. E. Cade & Son Ltd.* [1992] B.C.L.C. 213, 227.

30 See further paras. 29 and 30 of the Court of Appeal's judgment in *Taylor Goodchild Ltd v. Taylor and Another* [2021] EWCA Civ 1135 for a discussion of relevant case law in which the courts have emphasised the breadth of CA 2006, section 996 (Part 30).

© Law Business Research 2021

management is required. In circumstances where a buy-out order is sought, the court will normally determine issues necessary to decide whether a buy-out order should be made at a liability hearing, and only proceed to a quantum hearing if it has been determined that a buy-out order should be made.

34.4.3 Practical considerations

Typically, derivative claims and unfair prejudice petitions are brought by minority shareholders.[31] There are a number of practical advantages for such shareholders to bringing an unfair prejudice petition instead of a derivative claim. These include the broad grounds for relief, the flexible nature of the relief and the fact that there are fewer procedural hurdles to overcome. There may be significant disadvantages in bringing a derivative claim: the initial procedural phases can be costly, and relief must be sought on behalf of the company. However, in certain circumstances a derivative claim may still be the most appropriate route for shareholders (for example, in the context of public companies, where a finding of unfair prejudice may be less likely).

In a derivative action, the court may order the company, for whose benefit the action was brought, to indemnify the claimant against the costs it reasonably incurs. By contrast, in unfair prejudice proceedings, the company is not usually ordered to pay any costs.

The company may be required to give disclosure in the context of derivative claims and unfair prejudice petitions. A shareholder will be entitled to disclosure of documents obtained by the company in the course of the company's administration (where relevant), including advice by solicitors to the company about its affairs, but not where that advice relates to hostile proceedings between the company and its shareholders.

34.5 Securities litigation

As noted above, securities litigation[32] in England and Wales is relatively under-developed in comparison with the position in the United States. However, there are a number of ways in which investors in securities can seek relief before the English courts, and in recent years there has been an increase in the volume of such litigation, due in part to the growing role of third-party litigation funders and specialist claimant law firms.

Section 90 of FSMA makes persons (listed companies (issuers) and individuals within issuers) who are responsible for listing particulars or prospectuses liable to pay compensation for any untrue or misleading statement in the particulars, and for certain omissions from the particulars, to any person who has acquired securities to which the particulars relate and has suffered loss as a result of the statement or omission. A number of exemptions from

31 See further *Minority Shareholders: Law, Practice and Procedure*, Victor Joffe QC, David Drake, Giles Richardson, Daniel Lightman and Timothy Collingwood (6th ed. 2018).

32 See further *The Securities Litigation Review* (ed. William Savitt, 6th ed. 2020).

© Law Business Research 2021

such liability are set out in Schedule 10 of FSMA (for instance, where the defendant reasonably believed that the particular statement was true and not misleading, and continued in this belief until the relevant securities were acquired). Section 90A of FSMA applies more broadly to other categories of published information relating to securities, making an issuer liable to pay compensation to investors who suffer loss in respect of those securities as a result of a misleading statement or dishonest omission in that information, or a dishonest delay in publishing information (although liability under section 90A is in some respects more restricted than under section 90 – for instance, the standard of fault under section 90A is higher, and it is necessary to show reliance).[33] There is an increasing tendency for these cases to follow when there has been a significant investigation issue ostensibly linked to a fall in the share price and deferred prosecution agreement (DPA). In the financial services sector, private persons who suffer loss (such as purchasers of insurance products or investments) as a result of a breach by an authorised financial services firm of certain FCA rules can bring a claim for civil damages under section 138D of FSMA. The FCA determines which of its rules give rise to this cause of action, and this is set out in each chapter of the FCA Handbook. There has been some debate in the public domain about whether the UK government should create a new civil duty of care owed by financial services firms to consumers who could bring private claims in a broader range of scenarios. To date, the FCA has rejected that approach in favour of a proposal to create a new regulatory principle for consumer protection. There has also been discussion of extending section 138D to include claims for breaches of the FCA's Principles for Businesses. In its most recent consultation document, at the time of writing, the FCA is consulting only on whether to extend section 138D to include the proposed Consumer Principle.[34] The PRA also has the power under section 138D to provide that certain of its rules are subject to a similar right of action by private persons. Further, a number of other provisions in FSMA (for example, sections 26, 27 and 30) can render agreements or transactions unenforceable, and give rights to recover money or other property and to obtain compensation, where the circumstances in which those agreements or transactions were entered into contravene certain rules in FSMA, for instance, if necessary authorisation from the FCA has not been obtained.

Aggrieved investors may be able to bring other civil actions against financial services firms, in addition to claims under FSMA. Misrepresentation claims pursuant to section 2(1) of the Misrepresentation Act 1967 may be available to investors in circumstances where the investor enters into a contract in reliance on a misrepresentation made to them by another party to the contract, which causes loss, and where the representor did not have a reasonable belief at the

33 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch) was a high-profile case involving claims under the FSMA, s.90; in more recent litigation arising out of an overstatement of expected profits by Tesco plc in 2014, claims have been made under FSMA, s.90A.

34 FCA Consultation Paper CP21/13, 'A New Consumer Duty', Chapter 5.

© Law Business Research 2021

time the contract was made that the facts represented were true. Investors may also be able to bring a negligent misstatement claim (in circumstances where a duty of care is owed to the investor, that duty has been breached and that breach causes the investor to suffer recoverable loss), or a claim based on the tort of deceit (which requires, among other things, proof that the defendant knowingly or recklessly made a false representation).

34.6 Other private litigation

34.6.1 'Tainted' contracts

Conduct that is illegal or contrary to public policy (and that may well be the subject of an investigation) may 'taint' contracts entered into by a company.

The common law doctrine of illegality may prevent a party to a contract tainted by illegal conduct from enforcing their contractual rights and remedies in certain circumstances. Historically, the law in this area has been complicated and unclear, but it was reconsidered by nine Supreme Court justices in the case of *Patel v. Mirza*.[35] The majority held that the essential rationale underpinning the illegality doctrine is that it would be contrary to the public interest to enforce a claim if to do so would harm the integrity of the legal system. They identified the following three factors, which must be taken into account when considering whether to allow a claim that is in some way tainted by illegality:

- the underlying purpose of the prohibition that has been transgressed, and whether that purpose would be enhanced by denial of the claim;
- any other relevant public policy on which the denial of the claim may have an impact; and
- whether denial of the claim would be a proportionate response to the illegality. When considering proportionality, the majority held that (among other things) the seriousness of the conduct, its centrality to the contract, whether it was intentional and whether there was a marked disparity in the parties' respective culpability may potentially be relevant.

This approach was criticised by the minority, however, on the basis that it was too vague and too wide, converting a legal principle into the exercise of judicial discretion. It remains to be seen how the doctrine will develop in light of this important case.[36] For instance, in some more recent decisions, the courts have continued to have reference to case law that pre-dates *Patel*.[37]

35 [2016] UKSC 42.

36 See, e.g., *Stoffel & Co v. Grondona* [2020] UKSC 42.

37 See, e.g., *Henderson v. Dorset Healthcare University NHS Foundation Trust* [2018] EWCA Civ 1841 (appeals to Court of Appeal and Supreme Court both dismissed (*Henderson v. Dorset Healthcare University NHS Foundation Trust* UKSC 2018/0200)).

© Law Business Research 2021

Civil law bribery

If bribery has occurred, then a number of particular civil law consequences may also follow. Civil law bribery[38] arises in the context of agency relationships, where an agent receives a benefit that puts them in a position where their duty (to their principal) and their (personal) interest conflict. There must be a sufficient relationship of trust and confidence between the agent and principal.[39] The benefit does not necessarily have to be monetary, or provided directly to the agent, and there is no need to prove motive, inducement or loss up to the amount of the bribe. The bribe need not be linked to a particular transaction (provided the agent is tainted by bribery at the time of the relevant transaction between the briber and the principal), and it may taint subsequent transactions. An arrangement will not constitute a bribe in the absence of secrecy, although it may still amount to a breach of fiduciary duty on the part of the agent if the principal's fully informed consent is not obtained.

A variety of alternative remedies are available to a principal faced with civil law bribery.

As against the bribed agent

- If the bribe has been paid to the agent, the principal is entitled to recover the amount of the bribe (at common law, in an action for money had and received), regardless of whether the principal elects to rescind any 'tainted' contracts. The proceeds of bribe-taking (which comprise money or other property) will also be held on trust for the principal, and the principal will have a proprietary remedy in respect of them.
- In the alternative, the principal can claim damages in tort in respect of loss sustained by the principal in consequence of entering into any 'tainted' contracts.
- There may also be other consequences for the agent (including in connection with their contractual relationship with the principal).

As against the briber

- The briber is jointly and severally liable with the bribed agent in respect of the amount of the bribe, which the principal can claim in a common law action for money had and received.
- In the alternative, the briber is also jointly and severally liable with the bribed agent to the principal for damages in tort (see above).
- The principal may have an action for dishonest assistance in a breach of fiduciary duty against the briber.
- Other remedies may be available against the briber (or others) depending on the particular circumstances of the case.

38 See further *Bowstead and Reynolds on Agency* (ed. Peter Watts QC, 22nd ed. 2020).

39 As discussed in *Richard Conway & Deborah Conway v. Prince Arthur Ikpechukwu Eze* [2019] EWCA Civ 88.

© Law Business Research 2021

Note that double recovery by the principal from the bribed agent and the briber will not be permitted.

If it can be established that bribery has occurred, then the principal is usually entitled to rescind contracts 'tainted' by the bribery provided that the bribe was paid without the knowledge and consent of the principal.[40] If the principal elects to rescind a 'tainted' contract, they remain entitled to recover the bribe, and they are not bound to give credit in the rescission for the amount of any bribe recovered. If the agent is bribed during the course of performance of a contract (i.e., after it has been entered into), then the principal may bring it to an end as from the moment of discovery (i.e., for the future); and the same will apply if bribery was effected at the time a 'tainted' contract was entered into, but (for some reason) rescission *ab initio* is impossible. Where an arrangement would have constituted bribery, but the principal is aware of it (so there is no secrecy) although the principal's fully informed consent has not been obtained, then the court may award rescission of 'tainted' contracts as a discretionary remedy, if it is just and proportionate to do so.

Where bribes have been paid to the detriment of a third-party competitor, it has been suggested that both the briber and the company that awards the contract to the briber could be liable to the unsuccessful competitor. Further, if the contract involves a public authority, the unsuccessful competitor may have an action for misfeasance in public office.

A contract to commit bribery (as opposed to a contract procured by bribery) is 'tainted' by illegality, in the sense that it is illegal in performance, and is unenforceable.

34.6.2 Specific provisions in commercial contracts

Parties often include specific provisions in their commercial contracts (including finance documents) aimed at preventing, or providing contractual protection in relation to, illegal behaviour (in particular, corruption) involving a party to the agreement. Accordingly, the fact of an investigation (or related proceedings), or conduct that is the subject of an investigation, may have adverse contractual consequences for a company. These will naturally depend on the nature of both the investigation itself and the specific conduct under investigation, as well as the provisions of the contractual documentation. However, by way of illustration, many commercial contracts contain:

- obligations:
  - to comply with certain applicable laws and regulations;
  - to have in place and comply with specified policies (such as data protection, cybersecurity, anti-slavery and human trafficking or anti-bribery and corruption policies);
  - to maintain accurate records of payments made in relation to the contract;

40 See further *Wood v. Commercial First Business Ltd (in Liquidation) and Others* [2021] EWCA Civ 471.

© Law Business Research 2021

  - relating to data protection (for example, to prevent damage, or unauthorised or unlawful access, to relevant data);
  - in relation to subcontractors (for instance, to ensure that subcontractors comply with requirements equivalent to those imposed on the company), and that may impose responsibility on the company for any non-compliance by a subcontractor with such requirements;
  - to report generally on compliance to contractual counterparties on a continuing basis, which could include requiring the provision of a confirmation signed by an officer of the company. Audit rights may also be granted to contractual counterparties; and
  - to report the occurrence of certain events to contractual counterparties. These could include dealing with a public official in connection with the performance of the contract, receiving a request for a payment (or other advantage) in connection with the performance of the contract, or the commencement (or threat) of an investigation into the activities of the company;
- representations (given by the company, and that may be repeated) that it has not been investigated for or convicted of certain offences (and that no proceedings or investigations are pending or threatened), or that relate to the accuracy and completeness of information provided to contractual counterparties;
- termination rights for contractual counterparties if the company breaches (or, potentially, if the contractual counterparty reasonably suspects a breach of) certain obligations, or if the company makes a false representation or is convicted of certain offences; and
- indemnities (for the benefit of contractual counterparties) in respect of loss suffered as a result of a certain breaches of the contract by the company.[41]

A company may face parallel litigation brought by its contractual counterparties in reliance on such provisions. A company may also be able to invoke such provisions against its contractual counterparties, although where a company is under investigation it may not wish to take the position in civil proceedings that its counterparty has engaged in illegal activity if the company is also exposed for its counterparty's conduct.

Mergers, acquisitions and investments 34.6.3

Mergers, acquisitions and investments[42] can present particular risks for companies. Illegal behaviour in the target (or its subsidiaries, or other related companies and persons) may have various negative consequences for an acquiring entity,

41 An indemnity against a criminal liability may, however, be unenforceable for public policy reasons. See, for example, *Beresford v. Royal Insurance Co Ltd* [1938] AC 586.

42 See further *Anti-Bribery Due Diligence for Transactions: Guidance for Anti-Bribery Due Diligence in Mergers, Acquisitions and Investments*, Transparency International UK (2012).

© Law Business Research 2021

which can include (1) financial consequences (for example, the target may have been overvalued), (2) legal consequences (both civil and criminal) for the target, the acquiring entity and relevant individuals (including officers of both entities), along with associated legal costs and (3) other practical consequences (for example, reputational damage, which may have a consequent effect on business).[43]

As a result, acquiring entities will often take precautions to minimise these risks. Typically, these include:

- conducting proportionate pre- and post-acquisition due diligence of the target and its business;
- implementing compliance programmes; and
- including appropriate protections in the relevant contractual documentation.

In relation to the latter, warranties, representations and indemnities[44] designed to provide such protection are frequently included in share purchase agreements. The scope of protection will depend on the particular provisions negotiated, but they can be widely drafted, such that they encompass the conduct of, for example:

- the target and its subsidiaries;
- directors, officers, employees, significant shareholders, affiliates, agents, and distributors of the target and its subsidiaries;
- those associated with or acting on behalf of the target and its subsidiaries; and
- those who perform services for or on behalf of the target and its subsidiaries,

and may cover areas such as:

- compliance with laws generally;
- compliance with anti-money laundering laws and standards;
- compliance with anti-bribery and corruption laws and standards;
- debarment from public contracts;
- sanctions (including whether such persons are, have been, or are likely to become, subject to sanctions); and
- whether such persons are (or have been) subject to an investigation or any proceedings, or whether an investigation or any proceedings in respect of such persons are pending, threatened, contemplated, or even likely.

Accordingly, the existence of an investigation (or related proceedings), or conduct that is the subject of an investigation, may give the acquiring entity contractual rights, which it can seek to enforce (including through litigation or arbitration). Again, however, care may need to be taken in doing so, for the reasons given in Section 34.6.2.

43 Companies should also be aware of the risk that illegal behaviour (for example, bribery) may occur during the merger, acquisition or investment transaction.

44 However, see supra note 41, in relation to indemnities against criminal liability.

© Law Business Research 2021

Defamation proceedings 34.6.4

A company may face defamation actions[45] brought by individuals arising from internal investigations carried out by the company. In particular, issues may arise if it becomes necessary to negotiate an exit from the organisation for individuals involved or implicated in conduct that was the subject of an investigation.

The law of defamation is concerned with the protection of reputation. It covers the torts of libel (which concerns more permanent forms of publication) and slander (which concerns more transient forms of publication, such as speech, and generally is actionable only if special damage can be shown).

Broadly speaking, a defamatory statement is one whose publication has caused, or is likely to cause, serious harm to the claimant's reputation, although a number of different tests have been utilised by the courts when determining whether a statement is defamatory. The statement must have been published (communicated) to a third party, and each publication will amount to a separate cause of action. Liability for publication extends to those who participate in or authorise publication, and those who republish or repeat the relevant statement are liable as if the statement originated from them. However, defences are available in certain circumstances to persons who publish statements and who are not the author, editor or publisher (in the sense of being a commercial publisher) of the relevant statement; as well as to website operators, if they can show that the relevant statement was posted on the website by another.

A number of defences may be available to a company facing a defamation action. For example, it may be able to rely on absolute privilege, which will exist where a statement or conduct can fairly be said to be part of the process of investigating a crime (or a possible crime) with a view to a prosecution (or a possible prosecution) in respect of the matter being investigated. This applies to statements made by persons assisting an inquiry to investigators, and by investigators to those persons or to each other. Absolute privilege will also extend beyond the criminal context, to certain enquiries made in connection with proceedings before a tribunal, the proceedings of which are protected by absolute privilege (i.e., tribunals acting in a manner similar to that in which a court of justice acts). Accordingly, the provision of information by a company to the authorities in connection with an investigation is unlikely to expose that company to the risk of a defamation action. The defence of qualified privilege will also be available in circumstances where the maker of a statement has a legitimate interest or duty in making it to the recipient, and the recipient has a corresponding interest or duty in receiving it, provided the maker is not motivated by malice. This may apply to certain communications between an employer and their employees, or between employees, that relate to the employer's business.

45 See further *Gatley on Libel and Slander* (eds. Alastair Mullis and Richard Parkes QC, 12th ed. 2013).

© Law Business Research 2021

A company may also, in theory, be in a position to bring a defamation action against a whistleblower, given that the act of blowing the whistle will typically involve the publication of a statement that causes harm to reputation. Nonetheless, under the Defamation Act 2013, to satisfy the serious harm threshold, a company must show that the publication caused or is likely to cause serious financial loss. Whistleblowers may, however, be able to make out one or more possible defences to such a claim. In particular if the whistleblower can show that the statement was substantially true, this will generally constitute a defence to a defamation action. Whistleblowers may also benefit from the defence of absolute privilege (as set out above) or qualified privilege, provided that they are not motivated by malice. It is notable, however, that the Public Interest Disclosure Act 1998 does not provide protection from a defamation action for a whistleblower, although if such an action were brought by an employer this is likely to amount to a 'detriment' for the purposes of section 47B of Part V of the Employment Rights Act 1996.[46]

In addition, a company may be in a position to bring a defamation action in relation to press comment although litigation could have the effect of drawing attention to the allegation, which is seldom beneficial.

The primary remedy in defamation actions is the award of damages, and claimants may also seek an injunction against repetition of the publication complained of. In addition, the court may order the defendant to publish a summary of the court's judgment, and may also order others to stop distributing, selling or exhibiting material containing the relevant statement, or to remove the relevant statement from a website on which it is posted. Particular remedies are available where the claimant is granted summary relief.

Although in the past trial by jury was typical in defamation actions, the right to jury trial has recently been abolished in this context, and trial will now be by judge, save in exceptional circumstances.

34.6.5 Arbitration

Allegations of unlawful behaviour can have a significant impact in the context of international arbitration,[47] both before a tribunal itself and before national courts at the stage of recognition or enforcement of an award.

In the context of commercial arbitration, as in the context of civil ligation, allegations of unlawful conduct can impact parties' disputed rights and obligations under the applicable law in myriad ways. Should a regulatory body, for instance, determine a party's conduct to be unlawful, this might be taken into account by a tribunal in its consideration of claims of invalidity of a contract on grounds of illegality. In the context of recognition and enforcement of foreign arbitral awards, unlawful conduct may impact a court's assessment of a party's

46 See further *Whistleblowing: Law and Practice*, John Bowers QC, Martin Fodder, Jeremy Lewis and Jack Mitchell, 3rd ed. (2017).

47 See further *International Commercial Arbitration*, Gary Born, 3rd ed. (2020).

© Law Business Research 2021

claims to resist recognition or enforcement on the grounds set out in Article V of the New York Convention, for instance, on public policy grounds.[48]

A party's unlawful conduct can also have a significant impact in the context of determination of investor-state disputes arising under international treaties. In particular, numerous international tribunals have been faced with assessing allegations of investor misconduct, often involving corruption or bribery, in a variety of contexts. The findings of a domestic regulatory body, while compelling evidence of unlawful conduct under the law of the regulator's jurisdiction, are only one factor to be taken into account by an international tribunal. The consequences of unlawful conduct under a domestic law being proven to the satisfaction of an international tribunal will vary, and often depend to a large extent on the provisions of the treaty or other instrument under which the claim has been brought. In general terms, however, there is an emerging consensus in international practice that investment claims tainted by corruption or other unlawful conduct will be dismissed on grounds of inadmissibility (or, according to some tribunals, for lack of jurisdiction). Where investment treaty awards are governed by the New York Convention, the same considerations apply with respect to enforcement and recognition as for commercial awards.

Employment law and whistleblowing 34.6.6

Investigations can have employment law consequences for a company. Employees may seek to bring claims against their employers arising out of the subject matter of an investigation, or how the investigation is handled; conversely, an employer may wish to take action against an employee implicated in the conduct under investigation.

See Chapter 13 on employee rights

In addition, to the extent that allegations have been made by whistleblowers, companies under investigation or conducting investigations should carefully respect whistleblower rights (including a protection from being subject to a 'detriment' for blowing the whistle). For a disclosure to be protected, it must be made where the employee has a reasonable belief that the information tends to show breach of a legal obligation, is in the public interest and more than a personal issue for one individual,[49] and made to the employer or to a prescribed person. PRA regulated financial services firms must also comply with specific PRA and FCA whistleblowing rules covering policies, procedures and training on whistleblowing and, importantly, how they escalate and assess whistleblowing reports that meet the definition of 'reportable concerns' (which is very broad).

48 Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958, Article V(2)(b); Arbitration Act 1996, s.103(3).

49 As discussed in *Ibrahim v. HCA International Ltd* [2019] EWCA Civ 2007.

© Law Business Research 2021

34.6.7 Data breaches

The EU General Data Protection Regulation[50] applied in the United Kingdom from 25 May 2018 to 31 December 2020, and makes provision for the protection of natural persons with regard to the processing of personal data, and the free movement of such data. Following the United Kingdom's exit from the European Union, the provisions of the Regulation have been incorporated directly into UK law as the UK General Data Protection Regulation (UK GDPR) as a result of the European Union (Withdrawal) Act 2018 and Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

In addition to the penalties that may be imposed by supervisory authorities pursuant to the UK GDPR,[51] which can include an administrative fine of up to €20 million or up to 4 per cent of an undertaking's total worldwide annual turnover of the preceding financial year (whichever is higher) in respect of certain infringements, companies that are data controllers or processors may also face actions brought by data subjects in respect of infringements of their rights under the UK GDPR (data subjects may mandate representative organisations to bring actions on their behalf), as well as actions for compensation brought by any persons who have suffered damage as a result of an infringement of the UK GDPR.[52]

Relatedly, the UK GDPR also requires notification of certain personal data breaches to the competent supervisory authority without undue delay, and in certain circumstances communication to the data subject is also necessary.[53] In 2010, the FCA's predecessor body, the Financial Services Authority, fined Zurich Insurance £2.275 million after losing 46,000 policy holders' personal details.[54] Even in cases not involving personal data, companies may

50 Regulation (EU) 2016/679.

51 In the United Kingdom, the relevant authority is the Information Commissioner's Office.

52 See Regulation (EU) 2016/679, Articles 79, 80, 82 and 83. The courts have permitted a broad representative action against Google to proceed, in which the representative claimant sought compensation that was estimated as being in the range from £1 billion to £3 billion (*Lloyd v. Google LLC* [2018] EWHC 2599 (QB)). It was argued that Google had acted in breach of a duty imposed by the Data Protection Act 1998 (allegedly by secretly tracking the internet activity of Apple iPhone users, and using and selling the accumulated data). Following a successful appeal of the original High Court decision, the court found (among other things) that, on the facts alleged, relevant damage had been suffered because a person's control over their data could be valued, and that class members did have the same interest as they had lost control of their data over the same period and were not relying on any differentiating factors such as the amount of extracted date (*Lloyd v. Google LLC* [2018] EWCA Civ 1599). The Supreme Court granted Google permission to appeal the order and the hearing took place on 28 and 29 April 2021. At the time of writing, the Supreme Court's decision is still awaited.

53 ibid., Articles 33 and 34.

54 FSA Final Notice to Zurich Insurance Plc, UK Branch dated 19 August 2010.

© Law Business Research 2021

face significant regulatory consequences following cyberattacks. In 2018, the FCA imposed a fine of £16.4 million on Tesco Bank following a cyberattack in November 2016, for failings relating to the prevention of, and response to, a cyberattack that affected around 8,000 customers.[55]

Companies may also be responsible for data breaches by rogue employees. However, in 2020 it was held, in the context of a group action brought by more than 5,500 employees of a supermarket company whose personal information was disclosed by the actions of a disgruntled IT auditor employed by the company, that the company was not vicariously liable for the actions of that IT auditor. The Supreme Court held that the employee's actions were insufficiently connected to the activities that he had been assigned by the company and that he was seeking personal vengeance rather than furthering the company's business.[56]

Evidentiary issues 34.7

Reliance by the court on findings made by the authorities 34.7.1

Parties may seek to rely on findings made by the authorities in an investigation (such as a final notice from the FCA) in subsequent civil litigation. Objections may be raised to such reliance on the grounds of admissibility. As a matter of evidence, bare findings made in earlier proceedings are ordinarily inadmissible and excluded under what is known as the rule in *Hollington v. Hewthorn*,[57] although this controversial rule is subject to exceptions, and it has been held that a court can take into account the substance of underlying evidence as set out in prior decisions (giving it such weight as is appropriate).[58] In addition, a court may allow documents containing other relevant evidence, in addition to inadmissible findings, to be put before the court, with the judge taking into account that which is admissible and ignoring that which is inadmissible.[59] However, care should be taken when relying on regulatory findings in litigation. In *Property Alliance Group v. RBS*,[60] the court held that, while privileged material could be disclosed to the FCA on a limited waiver basis, in the circumstances, RBS had inadvertently waived privilege by making assertions in its defence about the scope of the FCA's subsequent findings. The court held that the bank's defence advanced a positive point that the regulator had not made a finding of misconduct in relation to GBP LIBOR and not simply repeated the public findings. In doing so, the bank had made the settlement discussions admissible evidence.

See Chapter 36 on privilege

55 FCA Final Notice to Tesco Personal Finance plc dated 1 October 2018.

56 *Wm Morrison Supermarkets Plc v. Various Claimants* [2020] UKSC 12.

57 *Hollington v. F Hewthorn & Co Ltd* [1943] KB 587.

58 See, e.g., *JSC BTA Bank v. Ablyazov & Anor* [2018] EWHC 1368 (Comm), [19].

59 *Rogers v. Hoyle* [2014] EWCA Civ 257, [53]–[55].

60 *Property Alliance Group Ltd v. Royal Bank of Scotland Plc* [2015] EWHC 1557 (Ch).

© Law Business Research 2021

Some investigations may result in criminal prosecutions and, potentially, convictions. In any subsequent civil proceedings, the fact of a UK conviction will be admissible in evidence for the purpose of proving, where relevant, that the convicted person committed the offence, and the information, complaint, indictment or charge sheet on which the person in question was convicted are admissible for the purpose of identifying the facts on which the conviction is based.[61] Where criminal proceedings follow civil proceedings, ordinarily findings of a civil court on the matters in issue in the criminal case will not be admissible in those subsequent criminal proceedings, although in some circumstances civil judgments may be admissible pursuant to the rules concerning evidence of bad character.

In addition, if a company enters into a DPA with a prosecutor, this must contain a statement of facts relating to the alleged offence and the company will be required to admit the contents and meaning of key documents referred to in the statement of facts.[62] Parties who bring civil litigation against the company may seek to rely on the contents of a DPA statement of facts as having the status of admissions by the company and may also seek disclosure of any underlying documents.

Certain specific rules apply in the competition law context. While the United Kingdom was an EU Member State, the High Court or CAT could not, under EU law, make determinations that conflicted with EU jurisprudence on certain competition law issues. The UK courts and competition authorities remain bound, when interpreting UK competition law, to ensure no inconsistency with EU competition case law that pre-dates the end of the Brexit transition period on 31 December 2020. They may, however, depart from such case law where it is considered appropriate in specific circumstances. UK courts are not bound by EU court rulings made after 31 December 2020 but may still have regard to them in appropriate cases. In these circumstances relevant EU court rulings may be accorded considerable weight in UK civil claims. In addition, the Competition Act 1998 (as amended) provides that findings of fact made by the CMA during the course of an investigation (which have not been appealed, or have been confirmed on appeal) that are relevant to an issue arising in certain competition law proceedings before the High Court or the CAT are binding on the parties to those proceedings, unless otherwise ordered. Further, where a claim is brought before the CAT or the High Court following an infringement decision by the CMA, (or the CAT on an appeal from a decision of the CMA), the CAT or the court is bound by that infringement decision once it has become final. The same is true in respect of European Commission infringement decisions in cases where the decision was made, or the investigation leading to the decision was commenced, before the end of the Brexit transition period.

61 Civil Evidence Act 1968, s.11.

62 Crime and Courts Act 2013, Schedule 17, para. 5(1); Deferred Prosecution Agreements Code of Practice, para. 6.1.

© Law Business Research 2021

Reliance by an authority on court findings 34.7.2

Matters that come to light during the course of civil litigation can have repercussions beyond the immediate context of those proceedings. They may draw the attention of the authorities, and there have been cases where authorities have relied on the findings of civil courts as grounds for taking action. For example, the FCA has previously prohibited individuals from carrying on regulated activities on the basis of findings in High Court judgments (in one instance, without conducting a separate investigation).[63] Accordingly, these risks may be relevant considerations for a company when considering and implementing its litigation strategy in civil proceedings. In addition, conflict and privilege issues may arise if the interests of the company and its employees are not aligned.

Collateral use of disclosed documents 34.7.3

English law can impose onerous disclosure obligations on parties to civil proceedings. Typically, parties are required to disclose documents on which they rely, and documents that adversely affect their case, adversely affect another party's case or that support another party's case (although the court may make an alternative order in relation to disclosure, and a pilot scheme initially rolled out for two years in January 2019 involving generally less expansive disclosure obligations to apply in the Business and Property Courts in England and Wales was recently extended until 31 December 2022[64]). In certain circumstances, parties may protect documents from inspection, for instance, on the grounds of privilege or the public interest. However, the confidentiality of a relevant document is not, of itself, a justification for refusing to disclose it, although it may be relevant to the exercise of the court's discretion to order disclosure. Although certain decisions of the English courts regarding the law of privilege had pointed towards a more restrictive interpretation of the scope

63 FCA Final Notice to Mr Anthony Verrier, dated 27 January 2014; FCA Final Notice to Mr Stephen Robert Allen, dated 14 April 2015; *Stephen Robert Allen v. The Financial Conduct Authority* [2014] UKUT 0348 (TCC).

64 See Disclosure Pilot for the Business and Property Courts Press Announcement, 31 December 2018, accessible on www.judiciary.co.uk; CPR Practice Direction 51U and the 122nd and 127th Practice Direction (PD) Updates, dated 21 July 2020 and 1 February 2021, respectively, which made amendments to PD 51U. The amendments made by the 127th update came into force on 6 April 2021. Further proposed changes were submitted by the Disclosure Working Group to the Civil Procedure Rule Committee on 9 July 2021 and were expected to come into force in October 2021 following a special meeting of the Civil Procedure Rule Committee in September 2021. These changes will constitute an extension of the pilot to 31 December 2022 (which came into effect on 7 August 2021) and further amendments to PD 51U.

© Law Business Research 2021

of the protection it offers,[65] the important judgment of the Court of Appeal in the *ENRC* case (concerning, in particular, the scope of litigation privilege in the context of a corruption investigation) suggests that this trend is beginning to change.[66]

As a result, a company involved in civil proceedings may be required to disclose sensitive documents to an opponent, including documents relevant to an investigation or even unprivileged investigation material. This includes correspondence with the regulator, although consideration should be given to whether the regulator needs to be informed of any such requirement in advance.

The impact of the invasion of a litigant's right to privacy and confidentiality that the obligation to give disclosure constitutes is mitigated to some extent by CPR Part 31.22, which provides that where a document has been disclosed to a party, that party may only use the document for the purpose of the proceedings in which it is disclosed, except where:

- the document has been read to or by the court, or referred to, at a hearing held in public (although the court may make an order restricting or prohibiting the use of such a document);
- the court gives permission; or
- the party who disclosed the document and the person to whom the document belongs agree.[67]

The court will only grant permission if there are special circumstances which constitute a cogent reason for permitting collateral use. Permission decisions are highly fact-sensitive. The proposed collateral use for the document will be relevant, and, depending on the proposed use, the court may carefully consider the particular documents in respect of which permission is sought.

If the court gives permission for collateral use, a party will be able to deploy the material outside the context of the civil proceedings. The court may make an order that they could be used in separate proceedings (including abroad). Once documents are moved outside the jurisdiction of the United Kingdom, there is a risk that they may be seized or that the party in possession of them may be compelled under local laws to produce them to third parties. Similar concerns about losing control over documents may arise where documents

65 See, for example, *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch), and the first-instance decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd* [2017] EWHC 1017.

66 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd* [2018] EWCA Civ 2006; see also *Bilta (UK) Ltd v. Royal Bank of Scotland* [2017] EWHC 3535 (Ch) (concerning litigation privilege) and *Property Alliance Group Limited v. The Royal Bank of Scotland Plc* [2015] EWHC 3187 (Ch) (in the legal advice privilege context).

67 See *Tchenguiz v. Grant Thornton* [2017] EWHC 310 (Comm) for the broad interpretation of collateral 'use' in relation to CPR Part 31.22, which includes, for example, reviewing documents for relevance; and see also *The ECU Group Plc v. HSBC Bank Plc & Ors* [2018] EWHC 3045, in which the judge emphasised the importance of the rule in CPR Part 31.22.

© Law Business Research 2021

have been provided to regulatory or enforcement authorities during the course of an investigation. Even where documents are shared with an authority on a conditional basis, the authority may share the documents with third parties if it believes it has a statutory duty to do so. There is also the risk that the authority will be required to disclose those documents if it becomes involved in civil proceedings.

Practical considerations 34.8

Coordination with investigations team 34.8.1

It is important that those within the company responsible for managing parallel civil litigation are in constant communication with the internal team responsible for dealing with investigations, to ensure that:

- a clear, holistic strategy is developed for managing the investigations and parallel civil proceedings, and anticipating areas of potential risk (e.g., possible civil claims that may arise but have not yet been commenced);
- both teams understand, and evaluate the risks of, new developments in both the criminal and civil spheres; and
- any proposed action by the company or associated persons, in the civil or criminal spheres, is carefully analysed to determine the potential repercussions for all other proceedings and investigations.

Similarly, the company's criminal and civil legal advisers should coordinate closely to ensure consistency of approach. Issues can arise, for instance, where:

- an authority seeks disclosure of privileged documents from the company in circumstances where the company may wish to assert privilege over those documents in subsequent civil proceedings;
- witnesses, whose testimony may be important for the company's case in civil proceedings, are under investigation, or have been classified as suspects, by the authorities, and have concerns about self-incrimination. Depending on the circumstances, employment proceedings may also be ongoing in respect of such individuals;
- pleading possible defences (such as illegality) in civil proceedings, which may strengthen the company's case in those proceedings but would undermine the position it has taken in relation to an investigation;
- (as part of DPA negotiations) there is a risk that matters which an authority seeks to include in an agreed statement of facts could be relied upon against the company in parallel civil proceedings. Conversely, any settlement agreement relating to civil proceedings may be disclosable to an authority as part of their investigation; or
- suspicious activity is identified in the course of civil proceedings (e.g., during disclosure), which the company is then obliged to disclose to the investigating authority.

See Chapter 7 on witness interviews

See Chapter 23 on negotiating global settlements

© Law Business Research 2021

34.8.2 Privilege waivers and disclosure obligations

During the course of an investigation, documents that attract privilege may be shown or provided to relevant authorities, often to demonstrate co-operation. These include not only privileged communications between lawyer and client but also documents, such as witness interview notes, generated by external counsel. Doing so will not necessarily constitute a general waiver of any privilege in those documents for the purposes of subsequent civil proceedings (particularly if it is made clear that this is done on a limited basis),[68] although it may lead to adverse consequences, as the company will lose a degree of control over the information in the documents. Particular care should be taken in cases involving multiple jurisdictions, as the effect of showing or providing a potentially privileged document to the authorities may vary depending on the law that governs questions of privilege.

34.9 Concurrent settlements

See Chapter 23 on negotiating global settlements

Difficult issues can arise for companies when attempting to negotiate settlement of global investigations, which can involve a variety of regulatory and prosecuting authorities across a range of jurisdictions. Parallel existing (or potential) civil litigation or arbitration adds a further layer of complexity to the analysis.

During settlement negotiations with the authorities, companies should be aware of the risk that the fact of a settlement, as well as any associated press coverage or documents (such as a statement of facts in a DPA), may raise awareness of potential civil claims, and in certain circumstances may even be relied upon to support such claims. This will be of particular concern in the competition law context, given the risk of follow-on actions. Accordingly, and to the extent possible, companies should avoid admitting liability as part of any negotiated settlement with the authorities; and, if an admission of liability is required, they should ensure that it is tightly circumscribed.

See Chapters 23 on negotiating global settlements and 36 on privilege

In addition, there is a risk that communications with the authorities made during the course of settlement negotiations will be disclosable in subsequent civil proceedings, although they may be protected from inspection by a right analogous to the 'without prejudice' rule.[69]

See Chapter 23 on negotiating global settlements

Settlement of civil claims can also carry risks for a company under investigation. There is a risk that settlement agreements entered into by the company may be disclosable in subsequent proceedings, or requested by an authority as part of their investigations. Companies should avoid admitting liability as part

68 In *Property Alliance Group Ltd v. Royal Bank of Scotland Plc* [2015] EWCH 1557 (Ch), the courts specifically recognised that privileged material shared with the FCA on an express limited waiver basis remained privileged against the rest of the world.

69 See, e.g., *Property Alliance Group Ltd v. Royal Bank of Scotland Plc* [2015] EWHC 1557 (Ch), in which the existence of without prejudice privilege in settlement negotiations with the FCA was recognised.

© Law Business Research 2021

of any negotiated civil settlement. In addition, authorities may perceive certain types of civil settlements (particularly those with witnesses for substantial sums) as suspicious. In the financial services space, firms should also be alive to the impact on civil claims on the outcome of past business reviews conducted under the supervision or awareness of the FCA.

In appropriate circumstances, it may be possible to settle civil claims on a multi-party basis. For instance, companies may try to reach collective settlements, which are available in respect of certain competition law claims (using the mechanism set out in the Competition Act 1998), or seek to utilise a collective redress scheme.

Concluding remarks 34.10

Cross-border investigations are complex and competing considerations need to be carefully weighed and managed. The prospect of parallel civil proceedings brings further complexity to an already difficult area. Such proceedings can present numerous and diverse challenges for a company subject to investigation – it may face a range of different types of action, on a number of fronts (for instance, involving shareholders, suppliers, customers or employees), which may impact an investigation, or be affected by an investigation, in a variety of ways. Companies will frequently be defendants in parallel proceedings and unable to exercise significant control over the existence or pace of the proceedings. They may at times be claimants out of necessity or to obtain a tactical advantage. It is important to give careful consideration at an early stage to potential parallel proceedings that may arise, and any effect they may have on an investigation (and vice versa), to enable possible tensions between investigations and parallel proceedings to be anticipated and managed effectively. There is no easy solution to the challenges presented by parallel civil proceedings. As noted above, it may be difficult to obtain a stay of them (without the consent of other parties to the proceedings), and settlements can give rise to their own particular complications.

© Law Business Research 2021

35

Parallel Civil Litigation: The US Perspective

David B Hennes, Lisa H Bebchick, Alexander B Simkin, Patrick T Roath and Jeel Oza[1]

35.1 Introduction

In the United States, when there are pending criminal and regulatory investigations, there are often also parallel civil proceedings brought by private individuals that pertain to the same or similar alleged conduct implicated by the investigations.

Parallel civil proceedings may precede the investigation, follow on from announced investigative findings or, as is frequently the case, arise during the course of the investigation as a result of public disclosures by a company about the existence or results of an investigation. These actions take a variety of forms, but class actions – in which a lead plaintiff seeks to prosecute claims on behalf of a large number of similarly situated plaintiffs – are the most prevalent in the United States. Class actions can introduce a range of complexities and pitfalls, including the prospect of increased alleged damages stemming from the aggregated impact to an entire class of purportedly aggrieved class members. Parallel private actions can also spur additional regulatory scrutiny in circumstances where, for example, a civil suit challenges conduct that was unknown to, or not the focus of, the relevant authorities.

Managing proceedings in this posture can present challenges. Parallel civil proceedings are governed by the procedural rules of the courts in which they are pending and the individual rules of the judges presiding over the cases. Because, among other things, civil proceedings can often proceed more quickly

1 David B Hennes and Lisa H Bebchick are partners, Alexander B Simkin is counsel, and Patrick T Roath and Jeel Oza are associates at Ropes & Gray LLP. The co-authors are grateful to Eugene Ingoglia and Anthony M Mansfield of Allen & Overy LLP for their contributions to previous editions of this chapter.

© Law Business Research 2021

than slower-moving investigations, tensions can arise with the investigative process, particularly with respect to the discovery process in civil litigation.

This chapter addresses the core challenges that arise when a company must manage parallel civil litigation in the United States at the same time as related investigations, and provides insight for companies and practitioners navigating the complicated issues that may arise under these circumstances.

First is a discussion about the most commonly invoked procedural manoeuvre by parties subject to parallel government or regulatory investigations and civil litigation: seeking to stay the private civil action. Next, the chapter summarises the forms of civil litigation that most often arise in the United States in this context and addresses considerations that may apply when dealing with each of them in the context of the competing private litigation and government-led investigative proceedings. Finally, the chapter provides additional insights and key takeaways for practitioners with respect to evidentiary issues, privilege concerns and business considerations, including potential insurance-related issues.

Stay of proceedings 35.2

Parties subject to parallel government investigations and civil proceedings frequently attempt to stay civil proceedings that relate to the same conduct under investigation. Pursuing a stay has appeal insofar as it allows a company under investigation to focus on the investigation, where the stakes are often higher, without the added distractions and complications from the parallel civil case. Of course, the plaintiff in the litigation sought to be stayed will typically oppose a stay in an attempt to gain additional leverage through the parallel proceedings.

Although a complete stay of parallel civil proceedings pending resolution of a government or regulatory investigation is often desirable, it can be difficult to obtain in practice. A court's decision concerning whether to grant a stay and the scope and timing of the stay is typically discretionary and a function of the individual judge's view as to how best to administer his or her own docket.[2]

Standard for issuing a stay 35.2.1

The precise standard that a court will apply when assessing whether to grant a stay varies by jurisdiction. In general, although courts in the United States are often sensitive to the potential prejudice to an entity or an individual named as a defendant, or the subject of a criminal proceeding, from being forced to proceed with parallel civil litigation about the same conduct, courts can nevertheless be hesitant to stay civil cases in their entirety just because an investigation is

2 See *Louis Vuitton Malletier S.A. v. LY USA, Inc.*, 676 F.3d 83, 97 to 99 (2d Cir. 2012). Note that this chapter endeavours to provide a representative summary of US law, which varies by jurisdiction. This chapter does not purport to address the potential variances across the various jurisdictions.

© Law Business Research 2021

pending. This is particularly the case when it is difficult to ascertain the precise scope and status of a government or regulatory investigation, as a court may be reluctant to stay a civil litigation that raises serious claims in deference to an investigation that may not be proceeding in a timely fashion.

Courts within the jurisdiction of the US Court of Appeals for the Second Circuit, which covers New York, have described a stay as an 'extraordinary remedy'.[3] The Second Circuit applies a standard[4] that is similar to other jurisdictions, which considers the following factors:

- the extent of the overlap between the issues in the criminal case and those in the civil case;
- the status of the criminal case, including whether the defendant has been indicted;
- the private interests of the plaintiff in the civil case proceeding expeditiously, weighed against the prejudice to the plaintiff caused by any delay associated with a stay;
- the private interests of and the burden to the defendant;
- the interests of the court; and
- the public interest.[5]

If a party's application for a stay is granted, the court may impose conditions and limitations on the stay, including as to scope and timing. For example, a court may allow discovery to proceed on certain topics or from certain parties. A court may also stay certain (or all) claims against certain parties, but allow other claims to proceed. A court could also enter a stay that expires after a fixed period, upon specific developments, or that includes deadlines for the parties

3 Id. at 98. The Second Circuit includes courts in New York, Connecticut and Vermont and its articulation of the standard is a representative mainstream position, and has been invoked by other circuit courts as well, see *SEC v. Desai*, 672 F. App'x 201, 205 n.5 (3d Cir. 1 Dec. 2016) (unpublished); *F.T.C. v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 627 (6th Cir. 8 Sep. 2014), in addition to being relied on by courts in numerous states and other federal jurisdictions, see, e.g., *Walker v. Wilburn*, 2015 WL 5873392, at *4 (N.D. Tex. 5 Oct. 2015); *Soe v. Sex Offender Registry Bd.*, 995 N.E.2d 73, 80 (Mass. 2013); *United States v. Ogbazion*, 2012 WL 4364306, at *1 (S.D. Ohio 24 Sep. 2012).

4 See *Louis Vuitton*, 676 F.3d at 97 to 99.

5 Other Circuits apply similar tests, with minor variations. See, e.g., *Microfinancial, Inc. v. Premier Holidays Int'l, Inc.*, 385 F.3d 72, 78 (1st Cir. 2004) (employing a seven-factor test assessing '(i) the interests of the civil plaintiff in proceeding expeditiously with the civil litigation, including the avoidance of any prejudice to the plaintiff should a delay transpire; (ii) the hardship to the defendant, including the burden placed upon him should the cases go forward in tandem; (iii) the convenience of both the civil and criminal courts; (iv) the interests of third parties; (v) the public interest . . . (vi) the good faith of the litigants (or the absence of it); and (vii) the status of the cases').

© Law Business Research 2021

to periodically update the court on the status of the parallel investigation or proceeding. In general, a party can apply to have a stay lifted at any time.[6]

Even when not a party, the government may seek to obtain a stay to protect the criminal process by, among other things, limiting a company's ability to use civil litigation to obtain broader discovery than is available in a criminal case. For instance, in a parallel civil case, putative or actual defendants in related criminal proceedings can seek the deposition testimony of key witnesses on which the government intends to rely in the criminal case, providing a significant advantage to defendants that would not otherwise exist in the absence of the civil case. Courts have discretion to impose full or partial stays of the civil proceedings in these circumstances.[7]

Seeking a stay to protect exercise of privilege against self-incrimination 35.2.2

Courts in the United States are likely to be particularly sensitive to requests to stay a parallel civil proceeding when an individual's constitutional right against self-incrimination is at risk of being compromised.[8]

The Fifth Amendment to the US Constitution protects natural persons from being 'compelled in any criminal case to be a witness against himself'.[9] The Fifth Amendment can also be invoked in civil cases when a witness's answers might incriminate her or him in concurrent or subsequent criminal proceedings. The privilege against self-incrimination is implicated in civil proceedings either when (1) pleadings, discovery or testimony in a civil proceeding could be used as an admission in a criminal proceeding,[10] or (2) admissions in a civil

6 See, e.g., *Lawrence v. Parker*, No. 2019 WL 5704594, at *2 (W.D. Mich. 16 Sep. 2019) (in context of parallel proceedings, court noted that '[i]f Defendants were concerned that some important evidence might be lost or otherwise unavailable, they could have moved to lift the stay').

7 See, e.g., *Doe v. Indyke*, 2020 WL 5518384, at *6 (S.D.N.Y. 14 Sep. 2020) (granting application for a partial stay in context of concurrent criminal investigation).

8 See, e.g., *United States v. All Assets of Statewide Auto Parts, Inc.*, 971 F.2d 896, 905 (2d Cir. 1992) ('because of the troublesome fifth amendment problems potentially generated by the government's use of the civil forfeiture statutes, district courts – absent some sort of extraordinary situation – should exercise their discretion to stay civil forfeiture proceedings pending the completion of related criminal proceedings against the claimants'); *C.E. Harris, Inc. v. Int'l Bhd. of Elec. Workers Local 595*, 2013 WL 6252485, at *5 (N.D. Cal. 3 Dec. 2013) ('Because our legal system provides for parallel criminal and civil proceedings, there may be a concern that parties can "use civil discovery as a pretext for gathering information useful for the criminal cases." To prevent this, "a district court may stay civil proceedings pending the outcome of parallel criminal proceedings, [but] such action is not required by the Constitution." Nonetheless, "a court should consider the extent to which the defendant's fifth amendment rights are implicated."') (citations omitted).

9 US Constitution, Fifth Amendment.

10 See *United States v. Barile*, 2007 WL 3534261, at *2 (N.D.N.Y. 13 Nov. 2007) ('The Fifth Amendment Protection against self-incrimination, "can be asserted in any proceeding, civil or criminal, administrative or judicial, investigatory or adjudicatory; and it protects against any

© Law Business Research 2021

proceeding could be deemed a waiver of the Fifth Amendment privilege in a manner that could be introduced as evidence in a criminal proceeding.[11]

Although the Fifth Amendment precludes adverse inferences in a criminal case, it does not forbid adverse inferences against parties to civil actions if a party declines to testify in response to probative evidence offered against it.[12] Likewise, an assertion of the Fifth Amendment by present or former employees can lead to an adverse inference of improper or wrongful conduct by a corporation in civil litigation.[13]

Because statements made by a party in a civil proceeding may be used against that party in a subsequent criminal proceeding, attorneys for individuals facing the possibility of parallel civil and criminal proceedings must remain cognisant of the fact that statements or testimony in a civil proceeding could be used against their clients in future criminal prosecutions. Note that although corporations may not invoke privilege against self-incrimination, courts have recognised that there may be circumstances in which it is impossible for a corporation to participate in civil discovery without implicating the Fifth Amendment rights of its corporate officers.[14]

---

disclosure which the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used"') (quoting *Kastigar v. United States*, 406 U.S. 441, 444 to 445 (1972)); see also *Guggenheim Capital, LLC v. Birnbaum*, 722 F.3d 444, 453 (2d Cir. 2013) (the Fifth Amendment 'privilege applies in civil proceedings only to disclosures reasonably believed to be used against defendant in a criminal case').

11 See *Highlander Holdings, Inc. v. Fellner*, 2020 WL 3498174, at *12 (S.D. Cal. 29 Jun. 2020) ('Generally, though, courts endorse the Second Circuit's admonition that a "testimonial waiver" of the Fifth Amendment privilege against self-incrimination based on the witness's prior statements "is not to be lightly inferred, and the courts accordingly indulge every reasonable presumption against finding a testimonial waiver"' (quoting *Klein v. Harris*, 667 F.2d 274, 287 (2d Cir. 1981)); see also *Klein*, 667 F.2d at 287 (articulating rule that a civil litigant waives privilege against self-incrimination when (1) the trier of fact is left with or prone to rely on a distorted view of the truth, and (2) the party has reason to believe that his or her actions would be interpreted as waiver).

12 See *Baxter v. Palmigiano*, 425 U.S. 308, 318 (1976) ('Our conclusion is consistent with the prevailing rule that the Fifth Amendment does not forbid adverse inferences against parties to civil actions when they refuse to testify in response to probative evidence offered against them').

13 See, e.g., *LiButti v. United States*, 107 F.3d 110, 113 (2d Cir. 1997) (vacating and remanding a case based on the lower court's failure to properly consider how an employee's invocation of the Fifth Amendment when questioned about his employment-related activity created an adverse inference against the corporate employer).

14 See, e.g., *United States v. Kordel*, 397 U.S. 1, 7 (1970) (noting that a party was 'not barred from asserting his privilege simply because the corporation had no privilege of its own'); *In re Twelve Grand Jury Subpoenas*, 908 F.3d 525, 528 (9th Cir. 2018) (holding that in *Braswell v. United States*, 487 U.S. 99, 104 (1988), 'the Supreme Court held that a corporate "custodian may not resist a subpoena for corporate records on Fifth Amendment grounds," regardless of whether the custodian could "show that his act of production would entail testimonial self-incrimination', but noting that '[i]n a footnote in Braswell, however, the Court left "open

© Law Business Research 2021

Potential types of parallel civil litigation 35.3

Class actions 35.3.1

Overview 35.3.1.1

In the United States, class actions are a common form of representative litigation through which a single plaintiff (or small group of plaintiffs) seeks to bring claims on behalf of a larger group of purportedly similarly situated persons. Class actions frequently arise in the securities and antitrust context where misconduct is alleged to have affected markets and large numbers of entities and individuals. In these circumstances, complex criminal and regulatory investigations often generate putative class actions.

Public records as a basis for class action filings 35.3.1.2

Class actions commonly arise in the United States following the public disclosure of reports of internal investigations, findings of regulators or the entry by a company or its executives into a plea or deferred prosecution agreement with the government. These documents can provide a road map for civil plaintiffs and can potentially be relied on as evidence in support of civil claims. When a class action survives a motion to dismiss and proceeds to discovery, it is common for a plaintiff to serve discovery requests that ask for (1) the company and any individual defendants to produce all materials that previously have been produced to the government, and (2) the government to produce documents that it collected in connection with its investigation.[15]

A class action plaintiff can also seek access to records produced to a federal agency, such as the Securities and Exchange Commission (SEC), outside the

---

the question whether the agency rationale supports compelling a custodian to produce corporate records when the custodian is able to establish, by showing for example that he is the sole employee and officer of the corporation, that the jury would inevitably conclude that he produced the records".'), cert. denied, 140 S. Ct. 289 (2019).

15 Parties request such information from the government pursuant to the regulatory framework established in the wake of the Supreme Court's ruling in *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951), relating to the authority of federal department heads to produce documents and determine whether department employees may testify in response to a subpoena. See 22 CFR § 1305. These are commonly referred to as '*Touhy* requests'. Federal circuits are split as to whether judicial review of a federal agency decision to resist a subpoena is governed by the Federal Rules of Civil Procedure or the Administrative Procedure Act's 'arbitrary and capricious' standard. See, e.g., *Wultz v. Bank of China Ltd*, 61 F. Supp. 3d 272, 279 (S.D.N.Y. 2013) ('Setting aside the details of the doctrinal disputes that underlie the various Circuits' positions, the practical effect of the disagreement is that the Second, Fourth and Tenth Circuits as a general rule give primacy to agencies' *Touhy* regulations over the Federal Rules of Civil Procedure when the two conflict, requiring litigants to exhaust their administrative remedies before moving to compel production from a governmental agency, while the D.C., Ninth, and Sixth Circuits generally give primacy to the Federal Rules over conflicting *Touhy* regulations.') (citations omitted).

© Law Business Research 2021

litigation process through a Freedom of Information Act (FOIA) request.[16] Most states have similar, but not identical, public access laws for state regulatory agencies.[17]

Notably, a number of exemptions to public disclosure apply to FOIA, including exemptions for records or information compiled for law enforcement purposes and documents relating to reports prepared by, on behalf of, or for the use of agencies that regulate financial institutions.[18] Although these FOIA exemptions are supposed to be narrowly construed in favour of disclosure, in practice, it is rare for FOIA requests to be granted during the pendency of an investigation. When a company or an individual is producing documents to the government, they should request confidential treatment under FOIA and request that the government provide notice if it receives a request for information from a third party; however, it is important to know that designation of information as confidential under FOIA does not necessarily render the information unavailable for purposes of discovery in civil litigation.[19]

35.3.1.3 Class action standards and procedural considerations

Federal class actions are governed by Rule 23 of the Federal Rules of Civil Procedure, which permits class certification when the purported class representative demonstrates that (1) the class is so numerous that joinder of all members is impracticable (i.e., numerosity), (2) there are common questions of law or fact among the entire class (i.e., commonality), (3) the claims of the proposed class representative are typical of the claims of the entire class (i.e., typicality), and (4) the proposed class representative will fairly and adequately represent the interests of the class (i.e., adequacy).[20] If these criteria are satisfied, the action must then fall within one of the following categories: (1) where the prosecution of separate actions runs the risk of inconsistent judgments that would result in incompatible standards of conduct for the

16 The Freedom of Information Act (FOIA), which is codified at 5 U.S.C. § 552, is a law that allows members of the public to seek access to information in the possession of the government.

17 See, e.g., New York's Freedom of Information Law, N.Y. Pub. Off. Law § Ch. 47, art. 6.

18 See 17 C.F.R. § 200.83 for a description of confidential treatment procedures under FOIA.

19 See, e.g., *Friedman v. Bache Halsey Stuart Shields, Inc.*, 738 F.2d 1336, 1344 (D.C. Cir. 2009) ('information unavailable under the FOIA is not necessarily unavailable through discovery'); see also *In re Subpoena Duces Tecum*, 439 F.3d 740, 753 to 754 (D.C. Cir. 2006) ('FOIA's exceptions to disclosure limit only the right to information conveyed pursuant to that statute and other limitations on the Commission's authority to publish information . . . [and] do not alter the Commission's duty to comply with lawful subpoenas after notice to the party whose information is sought') (citations omitted); *Atl. Specialty Ins. Co. v. Midwest Crane Repair*, LLC, 2020 WL 5118067, at *3 (D. Kan. 31 August 2020) ('This is not a FOIA case in which plaintiffs are seeking records directly from OSHA. And even if the OSHA documents were "exempt from disclosure to the general public under FOIA, it does not automatically follow the information is privileged . . . and thus not discoverable in civil litigation"' (citation omitted)).

20 Fed. R. Civ. P. 23(a).

© Law Business Research 2021

defendants, or adjudication with respect to individual class members would effectively impair the ability of other class members to protect their interests; (2) where injunctive or declaratory relief is sought and appropriate (and any monetary relief incidental); or (3) where common questions of fact or law predominate over any individualised ones, such that class treatment is the superior method for adjudication.[21]

Motions for class certification are often hotly contested. As a result of the evidentiary support that is required to support a class certification motion, these motions are most frequently, but not always, filed after completion of the discovery phase of the litigation. Once a judge agrees that the high evidentiary burden under the Rule 23 standard for class certification has been met and certifies a class, the stakes of the litigation, namely the potential benefits to plaintiffs (and their counsel) and the potential risks to defendants, are significantly increased because the class representative can now recover damages for the whole certified class and not just himself or herself.

Other than the issue of class certification, class action litigation proceeds in much the same way as other civil litigation brought by individual plaintiffs. Motions to dismiss at the pleading stage (i.e., before any class has been certified) that seek to have all claims in the case dismissed, or to narrow the claims at issue, are relatively common. Any claims surviving motions to dismiss then proceed to discovery, which generally requires, among other things, the exchange of documents by the parties and the taking and defending of depositions of witnesses under oath. Class action litigation can also involve the use of expert witnesses, with attendant expert disclosure and discovery obligations. The discovery phase of litigation can be burdensome, invasive and costly. As a result, it can frequently be worthwhile for defendants to evaluate whether a settlement may be possible for any claims that survive a motion to dismiss so as to avoid some or all of the burden and expense of discovery.

The discovery phase is typically followed by motions for summary judgment, where one or both sides seek judgment on any claims in which they contend there are no material facts in dispute.[22] Summary judgment motions are somewhat more common in cases that will be tried in front of a jury than those that will be tried in front of a judge, as some judges find it easier to proceed directly to trial rather than to spend time evaluating the often lengthy written summary judgment submissions and related exhibits. If the court denies summary judgment, the only remaining options are settlement or trial.

Given the cost and risks associated with litigating a class action trial for both sides, complex class action trials in the United States are relatively rare. Unlike civil litigation brought by an individual plaintiff, settlements of class action lawsuits must be approved by the court. All potential class members

21 Id.

22 Fed. R. Civ. P. 56(a) ('The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law').

© Law Business Research 2021

must also be given notice of any pending settlement and be afforded the opportunity to object or opt out of the proposed settlement. Should settlement occur prior to class certification, approval of the settlement is sought in conjunction with a streamlined class certification motion. In the event that a certain number of would-be class members opt out of the class, settlement agreements frequently afford defendants the right to rescind the settlement.

35.3.1.4 Class action statutory reforms

Numerous statutory reforms have had a meaningful impact on the filing and litigation of class action lawsuits in the United States.

The Class Action Fairness Act of 2005 (CAFA), for instance, has affected class action litigation in several notable respects. First, CAFA greatly expanded federal courts' jurisdiction over class actions by lowering the requirements for federal subject matter and diversity jurisdiction.[23] This change allows defendants to remove class actions from state courts to federal courts and consolidate multiple state proceedings into a single federal court class action. Lowering barriers to removal is generally viewed by defendants as helpful, as federal courts tend to have greater experience in overseeing class actions than their state counterparts, and thus there is more predictability in terms of how a case may proceed. Second, as a means of reducing perceived abuses, CAFA introduced a requirement that courts implement a heightened level of scrutiny to class action settlements.[24] Third, CAFA requires that designated federal and state officials for each state in which a class member resides be given notice of all settlements to afford them the opportunity to intervene as necessary to protect citizen class members.

In the context of securities litigation, two additional pieces of legislation were enacted to curtail frivolous class actions: (1) Private Securities Litigation Reform Act of 1995 (PSLRA);[25] and (2) Securities Litigation Uniform Standards Act of 1998 (SLUSA).[26] With respect to all securities litigation, including class actions, the PSLRA increased the evidentiary threshold necessary for a plaintiff to plead securities fraud by requiring that plaintiffs (1) plead false statements with particularity, (2) present evidence that the defendants knew that the alleged statements were false when made, and (3) allege loss causation. The PSLRA also stays discovery pending a court's resolution of a

23 28 U.S.C. §§ 1332(d) et seq. Under the Class Action Fairness Act of 2005 (CAFA), a class action satisfies the requirements for federal court jurisdiction so long as (1) the aggregate amount in controversy exceeds US$5 million, (2) there are at least 100 putative class members, and (3) there is at least one diverse plaintiff (i.e., 'minimal diversity').

24 For instance, when settlements result in net financial losses to class members, CAFA requires courts to ensure that the financial loss is substantially outweighed by non-financial benefits. Courts are also required to ensure that settlements do not discriminate against class members based on their geographical proximity to the court.

25 15 U.S.C. §§ 78u-4, 78u-5 et seq.

26 15 U.S.C. §§ 77p, 78bb et seq.

© Law Business Research 2021

motion to dismiss, challenging whether these requirements have been met. With respect to class action lawsuits specifically, the PSLRA granted judges greater authority to designate lead plaintiffs to act as class representatives.

SLUSA was enacted to combat efforts by plaintiffs to circumvent requirements of the PSLRA by filing a lawsuit in state court asserting state law claims, such as common law fraud. After the PSLRA was enacted, many plaintiffs sought to file class actions in state court to avoid the heightened evidentiary requirements of the PSLRA. As a result, SLUSA prohibits claims, whether filed in state or federal court, that allege fraud under state law in connection with the purchase or sale of securities from being pursued as a class action.[27]

Arbitration agreements in class actions 35.3.1.5

In recent years, the US Supreme Court has held that class action waivers in arbitration clauses found in employment and consumer agreements – which typically state that an employee agrees not to pursue resolution of disputes through a class action, but rather on an individual basis – are enforceable under the Federal Arbitration Act.[28] These types of arbitration agreements typically provide companies with a number of benefits, including that proceedings will remain confidential, and claimants (and their counsel) with less meritorious claims may be less inclined to pursue those claims on an individual basis. Companies should consider including class action waivers in their employment

27 There is an important exception to this general rule. The US Supreme Court has held that SLUSA does not prohibit state court class actions arising from a company's initial public offering, which is governed by the 1933 Securities Act, as distinct from a company's subsequent offerings, which are governed by the 1934 Securities and Exchange Act, and which are covered by SLUSA. See *Cyan Inc. v. Beaver Cnty. Employees Retirement Fund*, 138 S. Ct. 1061 (2018). Post-*Cyan*, state courts have split as to whether the provision of the PSLRA automatically staying discovery pending determination of a motion to dismiss applies in state court proceedings. Compare, e.g., *In re Dentsply Sirona, Inc.*, No. 155393/2018, 2019 WL 3526142, at *14 (N.Y. Sup. Ct. 2 Aug. 2019) (PSLRA's discovery stay provision is procedural and does not apply in state court proceedings) with *City of Livonia Retiree Health and Disability Benefits Plan v. Pitney Bowes Inc.*, No. X08 FST CV 18 6038160 S, 2019 WL 2293924, at *4 (Conn. Super. 15 May 2019) (PSLRA's discovery stay provision applies in state court proceedings). In July 2021, the US Supreme Court agreed to review a case that might have settled this question, but the parties settled the matter before a decision. See Petition for Writ of Certiorari at i, *Pivotal Software, Inc. v. Superior Court of CA*, No. 20-1541 (U.S. 3 May 2021).

28 See *DirecTV v. Imburgia*, 136 S. Ct. 463 (2015); *AT&T Mobility v. Concepcion*, 563 U.S. 333 (2011); see also *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612 (2018) (holding that arbitration agreements providing for individualized employee proceedings against employers must be enforced, notwithstanding provisions in statutory schemes to promote collective employment actions by employees); but see *Smith v. Bd. of Dirs. of Triad Mfg.*, 13 F.4th 613, 620–23 (7th Cir. 2021) (declining to enforce an otherwise valid arbitration agreement because doing so would have the effect of preventing plaintiffs from pursuing a statutory remedy expressly provided for in the ERISA statute). The Federal Arbitration Act is codified at 9 U.S.C. §§ 1 et seq.

© Law Business Research 2021

and consumer agreements and subjecting claims by employees and consumers to arbitration.

35.3.1.6 Class action opt-outs

An increasing trend in class action lawsuits is the prevalence of parallel 'opt-out' litigation, whereby an individual or entity that would otherwise be a member of the class opts out of the class action or otherwise brings a similar claim directly. The goal of opt-out plaintiffs is to try to negotiate a more favourable settlement than he or she would achieve if part of the class.

Opt-out plaintiffs are generally able to capitalise on the work done by class action counsel in an effort to reduce or share costs. They may also pursue their own discovery in an attempt to, for example, establish why their individual claims are stronger or more valuable than those belonging to the class more generally. For instance, in a stock drop case alleging material misrepresentations by company directors or officers, a large investor proceeding as an opt-out may seek to show that it relied on statements made by directors or officers to that investor directly, in addition to statements made to the investing public at large. There are a variety of other factors that may make an opt-out case more or less risky for a defendant, including the forum in which the case is proceeding, the legal claims asserted, or the identity and experience of the plaintiff 's counsel.

If a class action settles, the opt-out plaintiff generally has the option to accept the class settlement, proceed to litigate his or her own case individually (or in collaboration with other opt-out plaintiffs) or negotiate a separate settlement. An opt-out plaintiff 's ability to negotiate a separate settlement is often dependent on that plaintiff being able to credibly threaten to proceed to trial individually; otherwise, a defendant has little incentive to offer more than it offered to the rest of the class.

35.3.2 Derivative actions

35.3.2.1 Overview

In general, derivative lawsuits permit shareholders of a company to bring an action against a company's officers and directors, or controlling shareholders, seeking relief on the company's behalf.[29] Derivative suits often allege that the company officers and directors breached the fiduciary duties they owed to the company and caused the company harm.

35.3.2.2 Derivative standards and procedural considerations

Shareholder derivative lawsuits are filed pursuant to state law. Derivative suits filed in federal court are governed by state substantive law and the Federal Rules of Civil Procedure. Derivative lawsuits in the United States are most

29 See, e.g., 6 Del. C. § 17-1206 (authorising shareholder derivative suits); N.Y. Bus. Corp. L. § 626 (same).

© Law Business Research 2021

commonly filed in Delaware in light of the large number of companies that are incorporated in that jurisdiction.

In general, because a derivative claim is an asset of the company, a plaintiff who seeks to bring a derivative lawsuit must show either that the plaintiff has demanded that the company bring the suit in its own name and that the company refused to do so, or that such a demand would be futile.[30] When such a pre-suit demand is made, companies may form what is called a 'special litigation committee' to independently determine whether pursuing a shareholder's proposed claim is in the best interests of the company. A committee's determination that such a claim should not be brought can provide a strong defence for the individual defendants named in a shareholder derivative action.

In a derivative case, the plaintiff typically names the company as a nominal defendant.[31] Any ultimate recovery in a derivative lawsuit flows to the company.[32]

Indemnification and advancement 35.3.2.3

Corporate directors and officers are frequently entitled to indemnification and advancement under a company's by-laws and by state law.[33] Company by-laws typically provide that the company will advance (i.e., pay before final resolution of the litigation) attorneys' fees and costs to an individual director or officer who is named as a defendant in a lawsuit asserting claims arising out of his or her service to the company. Frequently a company's by-laws will afford an individual director or officer the right to advancement or indemnification not just to the minimum extent required under state law but to the fullest extent permitted under state law.

Directors and officers are not typically entitled to indemnification where bad faith conduct is proven, including in situations involving admissions of criminal acts or regulatory misconduct.[34] In these cases, whether and to what extent indemnification is available can become quite complex as parties

30 See, e.g., *Marx v. Akers*, 88 N.Y.2d 189 (N.Y. 1996); *Aronson v. Lewis*, 473 A.2d 405 (Del. 1984).

31 See, e.g., *Halebian v. Berv*, 644 F.3d 122, 127 n.4 (2d Cir. 2011) (citing *Meyer v. Fleming*, 327 U.S. 161, 167 (1946)); *Salzberg v. Sciabacucchi*, 227 A.3d 102 (Del. 2020).

32 See *Mesirov v. Enbridge Energy Co., Inc.*, No. CV 11314-VCS, 2018 WL 4182204, at *8 (Del. Ch. 29 Aug. 2018) (holding that, in a derivative case, '[t]he recovery – "restoration of the improperly reduced value" – flows to the corporation' (citation omitted)).

33 See, e.g., 8 Del. C. § 145 (authorising indemnification of corporate officers and directors); N.Y. Bus. Corp. L. § 722 (same).

34 For instance, under Delaware law, corporations are prohibited from indemnifying officers and directors found to have acted in bad faith. See 8 Del. C. § 145(a) ('A corporation shall have power to indemnify any person who was or is a party or is threatened to be made a party to any threatened, pending or completed action . . . *if the person acted in good faith* and in a manner the person reasonably believed to be in or not opposed to the best interests of the corporation' (emphasis added)); see also *Creel v. Ecolab, Inc.*, 2018 WL 5733382, at *5 (Del. Ch. 31 Oct. 2018) ('to obtain indemnification under Section 145(a), the director, officer, employee, or agent must show [*inter alia*] that . . . she "acted in good faith"').

© Law Business Research 2021

dispute whether amounts claimed are subject to indemnification in light of certain admissions. While court determinations regarding whether the alleged misconduct rose to the level of bad faith are still pending, directors and officers may have the right to advancement subject to a potential undertaking to repay the amount advanced. How these various disputes are resolved will depend on the specific by-laws at issue and the relevant statutory framework.

35.3.3 Commercial and contract litigation

In addition to class actions and derivative actions, parallel civil litigation also frequently arises from direct disputes, including contract claims and business torts. Commercial litigation may be predicated on a wide range of theories, including breach of contract, breach of fiduciary duty and employment disputes. Highlighted below are some of the more common types of direct civil litigation that is likely to be filed parallel to a government or regulatory investigation or proceeding.

35.3.3.1 Contract claims

Conduct that is illegal or contrary to public policy, and therefore may be the subject of a government investigation or prosecution, can also render commercial contracts void or voidable. The common law doctrine of illegality generally prohibits the enforcement of a contract tainted by illegality or misconduct. Of course, litigation outcomes in this area are highly dependent on the particular facts and circumstances, requiring courts to weigh a range of factors in determining whether to enforce a contract or specific contractual provision. Some misconduct can render a contract unenforceable by statute as well.[35]

Companies may also face parallel civil litigation brought to enforce a contract. Once government or regulatory investigations are made public, contractual counterparties may assert that the conduct giving rise to the investigation also breaches a term in a contract, including, for example, contractual representations by a company that it is in full compliance with particular laws, that it has robust anti-bribery and compliance procedures, or that it is not the subject of an active investigation or under threat of investigation.

35.3.3.2 Business torts

Government investigations may also result in the public disclosure of conduct that gives rise to alleged liability in the private civil tort context as well. For example, allegations from a government regulator could generate a claim

35 See *159 MP Corp. v. Redbridge Bedford, LLC*, 128 N.E.3d 128, 134 (N.Y. 2019) (holding that '[m]any rights implicate societal interests and, yet, they have been determined to be waivable [by contract,]' but identifying 'a limited group of public policy interests has been identified as sufficiently fundamental to outweigh the public policy favoring freedom of contract'); see also, e.g., CA Civ. Code. ch. 5 § 1608 ('If any part of a single consideration for one or more objects, or of several considerations for a single object, is unlawful, the entire contract is void').

© Law Business Research 2021

brought by commercial counterparties alleging that the same conduct constitutes fraud, tortious interference with commercial relations, or other unfair or deceptive business practices.[36]

Statutory claims 35.3.3.3

Conduct at issue in government or regulatory investigations can also give rise to claims premised on alleged violations of statutes that include a private cause of action. Statutory claims that may form the basis of a parallel civil claim include allegations that the defendant engaged in:

- unfair or deceptive business practices;[37]
- anticompetitive business collusion;[38]
- the submission of false claims to the government;[39] and
- the making of false statements in commercial advertising.[40]

Employment claims 35.3.3.4

Investigations may also have employee-related consequences for a company. For instance, employees may commence a lawsuit against employers arising from the underlying conduct being investigated. Employees may also bring claims for defamation based on statements their employer makes regarding that employee's conduct or character.[41] Employers may also pursue claims against

36 See, e.g., *In re Intuniv Antitrust Litig.*, 2020 WL 4274507, at *4 (D. Mass. 24 Jul. 2020) (private putative class action bringing antitrust claims alleging pharmaceutical companies colluded to harm generic drug manufacturers alongside 'Department of Justice's ongoing criminal investigation'); *Rio Tinto PLC v. Vale S.A.*, 2014 WL 7191250, at *1 (S.D.N.Y. 17 Dec. 2014) (fraud claims brought by 'multinational mining company' alleging that 'its principal competitor, entered into a conspiracy . . . to misappropriate . . . mining rights' amid concurrent federal criminal investigation); *A-Valey Engineers, Inc. v. Bd. of Chosen Freeholders of Cty. of Camden*, 106 F. Supp. 2d 711, 713 (D.N.J. 2000) (alleging bid-rigging in New Jersey public procurement led to civil lawsuit alleging tortious interference with business opportunities).

37 See, e.g., N.Y. Gen. Bus. Laws § 349; Mass. Gen. Laws ch. 93A § 9.

38 The Sherman Act, the key federal antitrust statute, includes a private right of action. 15 U.S.C. § 15.

39 The federal False Claims Act includes a private right of action. See 31 U.S.C. § 3730.

40 See, e.g., N.Y. Gen. Bus. Laws § 350-A ('False advertising').

41 See, e.g., *Ryniewicz v. Clarivate Analytics*, 803 F. App'x 858, 867 (6th Cir. 2020) (unpublished) (terminated employee brought defamation claim against former employer on the basis of 'certain statements made by representatives of [the former employer] to potential buyers in the context of [the former employer's] internal investigation [of the plaintiff]'); *Mott v. Anheuser-Busch, Inc.*, 910 F. Supp. 868, 874 to 878 (N.D.N.Y. 1995) (granting summary judgment in favour of employer on employee defamation claim stemming from employer's investigation and subsequent reporting of employee's illegal conduct, and finding that the investigation was conducted in a 'thorough and responsible manner' because it was initiated immediately following reports of wrongdoing, included interviews with all relevant parties and an extensive review of books and records, and was undertaken by a team including both inside and external counsel).

© Law Business Research 2021

employees implicated in the conduct under investigation. In situations where investigations involve an employee whistleblower, companies should also be mindful of whistleblower protections to avoid claims for breach of their rights.

35.4 Evidentiary issues

Concurrent civil litigation and government investigations raise potentially vexing issues related to the staging, timing and exposure of evidentiary findings. The evidentiary dilemmas run in both directions – implicating both evidence from the civil action that could play a role in the criminal or regulatory proceedings, and vice versa.

35.4.1 Reliance by civil litigants on regulatory findings

Litigants may seek to incorporate facts developed in a regulatory investigation into a subsequent or concurrent civil claim.

To the extent that facts are admitted by a company, for example, in a deferred prosecution agreement or a guilty plea, those facts may be admitted into evidence as party admissions under US evidentiary rules.[42] Deferred prosecution or plea agreements may also specifically prohibit a company from denying certain facts.[43] In addition, to the extent that a party discloses otherwise privileged information to the government in connection with a deferred prosecution or plea agreement, a civil litigant may argue that the party waived privilege as to that information and perhaps more generally, as discussed below.

---

42 A settlement with a civil regulator may be reached without the company (or the individual) admitting or denying the regulator's findings set forth in the settlement order. In this circumstance, the regulator's findings are generally inadmissible in subsequent civil litigation. See, e.g., *Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec.*, LLC, 797 F.3d 160, 179 n.11 (2d Cir. 2015) ('SEC orders like the one at issue here inadmissible to prove the facts of liability'); see also *Bowers v. NCAA*, 563 F. Supp. 2d 508, 536 (D.N.J. 2008) (holding Rule 408 'plainly applicable' to the consent decree at issue and refusing to allow the plaintiff to use a consent decree between the defendant and the Department of Justice as evidence of the defendant's liability for the conduct underlying the plaintiff's claim); *Carpenters Health & Welfare Fund v. Coca-Cola Co.*, 2008 U.S. Dist. LEXIS 112503, at *22 (N.D. Ga. 2008) (granting motion to exclude SEC civil consent order from evidence); *In re Blech Sec. Litig.*, 2003 WL 1610775, at *10 to 11 (S.D.N.Y. 2003) (finding SEC consent judgments inadmissible under Rule 408); *Safford v. St. Tammany Parish Fire Prot. Dist. No. 1*, 2003 WL 1873907, at *5 (E.D. La. 2003) (holding that consent decree cannot be used as evidence of prior liability).

43 See, e.g., SEC Deferred Prosecution Agreement, *In re: John Kullus* ¶ 9 (Jun. 2018), available at https://www.sec.gov/litigation/litreleases/2018/lr-24222-john-kollus-deferred-prosecution-agreement.pdf ('Respondent agrees not to take any action or to make or permit any public statement through present or future attorneys, employees, agents, or other persons authorized to speak for him, except in legal proceedings in which the Commission is not a party / in litigation or otherwise, denying, directly or indirectly, any aspect of this Agreement or creating the impression that the statements in Paragraph 6 of this Agreement are without factual basis').

© Law Business Research 2021

Reliance by regulators on findings by a court in civil litigation 35.4.2

Facts discovered and publicly disclosed during the course of civil litigation may also draw the attention of the government or regulators, which may rely on the findings in a civil case as grounds for commencing an investigation or taking some other enforcement action.

A civil defendant facing an actual or potential parallel government investigation should factor these risks into its consideration of how best to proceed with respect to the parallel civil proceedings.

Collateral use of disclosed documents 35.4.3

In the United States, the scope of discovery in civil cases is relatively broad. Parties in federal civil litigation must typically disclose all reasonably accessible relevant non-privileged evidence, whether helpful or harmful.[44] The purported confidentiality of a relevant document is not a justification for refusing to disclose it, although confidential documents can be afforded some level of protection from public disclosure by court-issued protective orders.[45]

As a result, companies or individuals involved in civil proceedings are frequently required to disclose sensitive documents to their adversary. If an adversary is aware of a government or regulatory investigation, it will typically demand production of any document that has been given to the government; in practice, these documents are often produced. In making this production to an adversary, a company should seek a protective order that requires, among other things, that the adversary maintain the information as confidential and refrain from using the information for any purpose other than litigation. However, even with the benefit of such a protective order, it can be challenging to maintain the confidentiality of any document or information used in connection with a summary judgment motion or at trial due to the policy in favour of open-court proceedings.[46]

---

44 Fed. R. Civ. P. 26(b)(1). Rule 26 'is liberally construed and is necessarily broad in scope', *MacCartney v. O'Dell*, 2018 WL 5023947, at *2 (S.D.N.Y. 2018), though '[o]f course, as in all matters relating to discovery, the district court has broad discretion to limit discovery in a prudential and proportionate way'; *EM Ltd. v. Republic of Argentina*, 695 F.3d 201, 207 (2d Cir. 2012).

45 Fed. R. Civ. P. 26(c); see also *Closed Joint Stock Co. 'CTC Network' v. Actava TV, Inc.*, 2016 WL 1364942, at *5 (S.D.N.Y. 28 Mar. 2016) ('An order limiting the use of discovery to the litigation in which it is produced "is particularly appropriate when the material at issue is private"' (quoting *Duling v. Gristede's Operating Corp.*, 266 F.R.D. 66, 77 (S.D.N.Y. 2010)).

46 See, e.g., *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 113 (2d Cir. 2006). Whether a court will 'allow documents to be filed under seal in connection with motions and court proceedings is a wholly separate inquiry governed by a different standard'. *Martinez v. City of New York*, 2018 WL 582321, at *1 (E.D.N.Y. 26 Jan. 2018) (quotations omitted). 'To determine whether it is appropriate to allow documents to be filed under seal, courts engage in a two-part inquiry. First, the court decides how strong a presumption of access a document deserves with reference to its role in the judicial process. Next, the court will "balance the

© Law Business Research 2021

35.4.4 Potential privilege waiver and disclosure obligations

During an investigation, documents entitled to privilege or work-product protection may be provided to relevant authorities, often to demonstrate co-operation.

These include not only privileged communications between attorney and client but also documents generated by external counsel, such as witness interview memoranda, which may be covered by the attorney work-product privilege. Depending on the applicable privilege law, which can vary materially from state to state and even between the federal Circuit Courts of Appeal, sharing such information will not necessarily constitute a general privilege waiver for the purposes of subsequent civil proceedings (particularly if it is made clear that the material was shared on a limited basis).[47] In cases involving multiple jurisdictions, it is critical that a company obtain advice on all potentially applicable privilege laws prior to sharing potentially privileged documents to the government, as the effect of providing a potentially privileged document to the authorities may vary depending on which law governs questions of privilege.

In addition, representation and privilege issues may arise if the interests of the company and its employees are not aligned. For example, company counsel may represent a key employee witness at deposition in a civil case, but in the context of a subsequent criminal investigation may be conflicted from continuing the representation should the employee's interests diverge from the company's interests,[48] such as if the company wishes to disclose misconduct to the government but the employee wishes to invoke his or her Fifth Amendment privilege against self-incrimination.

35.5 Additional practical considerations

It is helpful to consider additional practical considerations concerning the management of multi-track disputes, including (1) coordination between civil and investigatory response teams, (2) attempting to negotiate parallel settlements, (3) business events likely to give rise to parallel litigation, and (4) insurance considerations.

---

weight of that presumption, if any, with competing interests, namely, the private interests and concerns of judicial efficiency and law enforcement, to determine whether or not to seal a document.'" Id. (citations omitted).

47 As a condition to the disclosure of otherwise privileged information, a company may ask that a regulator stipulate that it will not assert a waiver of applicable privilege in any subsequent enforcement action. However, it is important to note that a stipulation by a regulator does not bind third parties.

48 See, e.g., N.Y. Unified Court System, Rules of Professional Conduct, Rule 1.7(a)(1) (a lawyer cannot concurrently represent two clients with differing interests).

© Law Business Research 2021

Coordination with internal investigations team 35.5.1

It is important that in-house teams responsible for managing parallel civil litigation are in regular communication with the internal team responsible for dealing with investigations, to ensure that:

- a clear, holistic strategy is developed for managing investigations and parallel civil proceedings and anticipating areas of potential risk;
- litigation teams are nimble and capable of responding in real time to new developments;
- both teams understand, and appreciate the risks of, new developments in both the criminal and civil contexts; and
- any proposed action by the company or associated persons, in the civil or criminal context, is carefully analysed to determine the potential repercussions for the related proceedings and investigations.

Issues can arise, for instance, where:

- factual admissions are made in civil proceedings (such as in an answer or in interrogatory responses) that may undermine the defence of the criminal case;
- an authority seeks disclosure of privileged documents from the company in circumstances where the company may wish to assert privilege over those documents in subsequent civil proceedings;
- witnesses, whose testimony may be important for the company's case in civil proceedings, are under investigation, or have been classified as subjects of criminal investigations by the government and have concerns about self-incrimination;
- pleading possible defences (such as illegality) in civil proceedings, which may strengthen the company's case in those proceedings but may undermine the position it has taken in relation to an investigation; or
- as part of deferred prosecution agreement negotiations, there is a risk that matters an authority seeks to include in an agreed statement of facts could be relied on in parallel civil proceedings against the company.

Close coordination is also necessary between the company's criminal and civil external legal advisers to ensure consistency of approach and strategic alignment.

Negotiating and executing concurrent settlements 35.5.2

Difficult issues may arise for companies when attempting to negotiate a global settlement of investigations, which can involve a variety of regulatory and prosecuting authorities across a range of different jurisdictions. Parallel existing (or potential) civil litigation adds a further layer of complexity to the analysis.

During settlement negotiations with government authorities, companies should be aware of the risk that a settlement, as well as any associated press coverage or documents (such as a statement of facts in a deferred prosecution agreement), may raise awareness of potential civil claims, and that documents pertaining to the negotiation of a settlement, including communications with

© Law Business Research 2021

the relevant authorities and drafts of the settlement, may be discoverable by plaintiffs in any such civil action.[49] Accordingly, to the extent possible, companies should avoid admitting liability as part of any negotiated settlement with the government. If an admission of liability is required, companies should ensure that it is narrowly tailored. Companies should also consider what they convey during the course of settlement discussions and how they communicate information.

There are also risks attendant to the settlement of civil claims for a company under investigation, in particular class action settlements, which are necessarily public. Companies should avoid admitting fault or liability in connection with any negotiated civil settlement. In addition, the government may perceive certain types of civil settlements (particularly settlements with potential witnesses for substantial sums) as suspect.

35.5.3 Business events likely to give rise to parallel litigation

There is a heightened risk associated with certain corporate events generating potential parallel regulatory investigations and civil litigation. In particular, mergers and acquisitions can present heightened risks for these types of developments and companies engaging in such transactions should be particularly attuned to the potential risks. In addition, potential purchasers of or investors in business entities should evaluate the risk that a target company acted in an illegal fashion and that any corresponding liability associated with the resolution of proceedings arising from the misconduct could be acquired in connection with the transaction.

Historical illegal conduct by a target company (or its subsidiaries, or other related companies and persons) may have various negative consequences for an acquiring entity, which can include financial consequences (for example, the target may have been overvalued); legal consequences (both civil and criminal) for the target, the acquiring entity and relevant individuals (including officers of both entities),[50] with associated legal costs; and other practical consequences (for example, reputational damage, which may have a consequent effect on business).

---

49 Federal Rule of Evidence 408 limits the admissibility of evidence pertaining to settlements and their negotiation. It does not, however, speak to the discoverability of such information. Numerous courts have addressed the availability of a 'settlement privilege' to limit discovery of settlement-related documents, reaching different conclusions. Compare *Stockman v. Oakcrest Dental Center P.C.*, 480 F.3d 791 (6th Cir. 2007) (applying settlement privilege) with *Morse/Diesel, Inc. v. Fidelity & Deposit Co. of Maryland*, 122 F.R.D. 447, 449 (S.D.N.Y. 1988) (declining to recognise settlement privilege).

50 In formal guidance, the US Department of Justice (DOJ) addressed factors that may be relevant in determining whether and how the DOJ would seek to impose post-acquisition successor liability on an acquirer for pre-acquisition Foreign Corrupt Practices Act (FCPA) violations by its target. See DOJ, 'Foreign Corrupt Practices Act Review', No. 14-02 (7 November 2014). The DOJ 'encourages companies engaging in mergers and acquisitions to (1) conduct thorough risk-based FCPA and anti-corruption due diligence; (2) implement the acquiring company's code of conduct and anti-corruption policies as quickly as practicable;

© Law Business Research 2021

As a result, acquiring entities should take appropriate precautions to minimise these risks. Typically, these include conducting proportionate, risk-tailored pre- and post-acquisition due diligence of the target and its business, including a review of material aspects of the target's business dealings and third-party contracts, implementing compliance programmes, and including appropriate protections in the relevant contractual documentation.

Contractual provisions, such as representations, indemnities and warranties designed to provide protection should also be incorporated into purchase agreements. The scope of protection will depend on the particular provisions negotiated, but they can be widely drafted, such that they explicitly encompass:

- the conduct of the target company and its subsidiaries, and of all directors, officers, employees, affiliates, agents and distributors of the target and its subsidiaries;
- compliance with laws generally, and more specifically compliance with anti-money laundering laws and standards, anti-bribery and corruption laws and standards, and sanctions laws (including whether any of the aforementioned persons are, have been, or are likely to become, subject to sanctions); and
- representations as to whether any of the aforementioned persons are, or have been, subject to an investigation or any proceedings, or whether an investigation or any proceedings in respect of those persons are pending, threatened, contemplated or even likely.

Accordingly, the fact of an investigation (or related proceedings), or conduct that is the subject of an investigation, may give the acquiring entity contractual rights it can later seek to enforce (including through litigation or arbitration). The acquiring entity should, therefore, review material aspects of the target's business dealings and third-party contracts for potential exposure, which may include consideration of the target's in-house and external legal advice relating to those dealings and contracts.[51]

Insurance considerations 35.5.4

The costs associated with defending civil litigation and investigative matters can be significant, particularly in the United States. Identifying any applicable

(3) conduct FCPA and other relevant training for the acquired entity's directors and employees, as well as third-party agents and partners; (4) conduct an FCPA-specific audit of the acquired entity as quickly as practicable; and (5) disclose to the Department any corrupt payments discovered during the due diligence process.' Id. at 3 to 4.

51 An acquiring company should be conscious, however, of the potential for a privilege waiver by the target company if such legal advice is shared outside the context of litigation. The law on this subject varies from state to state, but in New York, for example, pre-closing communications between counsel for a target company and its acquirer are not privileged unless they relate to pending or anticipated litigation. See *Ambac Assurance Corp. v. Countrywide Home Loans, Inc.*, 27 N.Y.3d 616 (2016).

© Law Business Research 2021

insurance policies and providing timely notice of potential claims under those policies is critical.

A company or individual facing parallel investigations and litigation should take steps to ascertain the existence, nature and terms of any potentially applicable insurance policies as early as possible. Key initial questions relate to:

- the coverage terms of the policy and whether the allegations in the regulatory investigation or civil lawsuit give rise to a potential claim under the policy;
- limits on the reimbursement of attorneys' fees and provisions allowing the insurer to assume defence of a matter;
- the liability period covered by the policy;
- provisions governing the time and nature of any claim made pursuant to the policy; and
- the amount of the deductible and policy limit per occurrence and per policy.

Although the terms of the applicable policies should control, it is often prudent to notify any potentially implicated insurers of the existence of a potential claim against the policy as early as is practicable. Managing the relationship with an insurer that is in the process of making a coverage determination or assessing whether to assume the defence of a litigation is important. Frequently, insureds or potential insureds will benefit by providing insurers with regular updates of developments and strategic decision-making with respect to key issues in the parallel actions.

In addition, it is not unusual to have parallel government investigations and civil litigation covered under the same insurance policy or tower of policies. In these circumstances, insureds should be particularly mindful of ensuring that their insurance resources are appropriately spent on the most important priorities, especially if there is a risk that there is inadequate insurance to cover the full range of government investigations and civil litigation. For example, an insured may not want to spend all its insurance asset on a civil litigation, leaving it with inadequate funds to properly defend a potential criminal proceeding.

These matters are complicated by the fact that, in cases of parallel proceedings, there can often be multiple different insured parties all covered under the same insurance policy or policies with potentially competing priorities. For example, an individual who has been personally sued in a civil litigation may prioritise settling the specific lawsuit against her or him even though the company or another insured may prioritise the settlement or defence of other claims or investigations. Although the wording of the insurance policy generally controls and the law can vary from state to state, in many instances, insurers are expected to pay covered claims in the order they are presented. This can, in certain circumstances and absent coordination, create a rush to access the insurance proceeds. Accordingly, coordination between and among potential co-defendants or investigation targets can be particularly important in the event of parallel investigations and civil litigation involving multiple insured parties.

© Law Business Research 2021

On the other hand, while uncommon, in some circumstances, a company or individual may consider foregoing insurance coverage or negotiating a compromise in the amount of insurance due from an insurer, so as to prevent an insurer from assuming the defence of a matter, especially where allowing an insurer to take control of the defence of a matter might diminish a person's ability to appropriately manage parallel claims.

In the event of a dispute between an insured and an insurer about coverage, an individual or entity can potentially find herself, himself or itself involved in parallel insurance coverage litigation in addition to the pending investigations and civil litigation. This, of course, raises and potentially magnifies many of the same issues addressed in this chapter. For example, an insurer may seek to deny coverage by attempting to prove the investigations or civil lawsuits were the result of intentional misconduct by an insured, which may be excluded from coverage, and which could also be in tension with the insured's criminal and civil defence strategy. As such, it is important to be mindful of all the potential ramifications when dealing with insurance in the context of parallel civil and criminal and regulator matters.

Conclusion 35.6

Appropriately managing parallel civil litigation and criminal and regulatory proceedings can present many potential challenges and hurdles. Handling the complications associated with competing parallel proceedings requires careful strategic decision-making and forethought. The insights covered in this chapter are intended to provide robust, practice-oriented guidance to those navigating these challenges.

© Law Business Research 2021

36

Privilege: The UK Perspective

Tamara Oppenheimer QC, Rebecca Loveridge and Samuel Rabinowitz[1]

36.1 Introduction

The law of privilege confers on persons the right to refuse to produce a document or to answer questions – including by a regulator or prosecuting authority. The two subcategories of legal professional privilege are (1) legal advice privilege and (2) litigation privilege. This chapter explains the basic principles applicable to these, having particular regard to the regulatory and investigatory context. It also addresses briefly two other types of privilege that may arise in the regulatory context, namely common interest privilege[2] and without prejudice privilege.

This chapter also discusses certain exceptions to privilege and the circumstances in which privilege can be lost or 'waived', either intentionally or inadvertently. The final section of the chapter addresses some more practical issues of how to maintain privilege in the regulatory and investigatory context.

1 Tamara Oppenheimer QC, Rebecca Loveridge and Samuel Rabinowitz are members of Fountain Court Chambers. The authors are grateful to Bankim Thanki QC for his contributions to previous editions of this chapter.

2 Common interest privilege (along with joint interest privilege) is traditionally analysed as a distinct category of privilege, although it depends on the existence of material to which either legal advice or litigation privilege applies.

© Law Business Research 2021

Legal professional privilege: general principles 36.2

The relevant distinction between legal advice privilege and litigation privilege is as follows:[3]

- Legal advice privilege is concerned with communications between lawyer and client for the purpose of giving or receiving legal advice or assistance,[4] in both the litigation and the non-litigious context.
- Litigation privilege is concerned with communications between a client or his or her lawyer and third parties for the purposes of litigation (whether anticipated or commenced).

Notwithstanding frequent misconceptions to the contrary, litigation privilege has no application to communications between lawyer and client, even where litigation is anticipated or has actually commenced: such communications will always fall within the ambit of legal advice privilege.[5]

Before turning to consider these two aspects of legal professional privilege separately, a number of general observations should be made.

The need for confidentiality 36.2.1

Privilege requires and protects the confidentiality of documents and exchanges. Confidentiality is therefore a necessary, but not a sufficient, condition for both limbs of legal professional privilege.[6] The question is whether a document has the necessary quality of confidence, such as to attract privilege. This is rarely problematic, as it can usually be inferred that communications between lawyers and their clients or with third parties in the context of actual or anticipated litigation have been impressed with confidence. Nevertheless, some communications may be regarded as lacking that character. Hence, in the context of legal advice privilege, the client's identity,[7] address[8] or the existence of the

3 *Waugh v. British Railways Board* [1980] AC 521, 541–42, HL (*per* Lord Edmund-Davies). The distinction set out in Lord Edmund-Davies' speech was applied by the Court of Appeal in *Re Highgrade Traders Ltd* [1984] BCLC 151, 164, 165 (*per* Oliver LJ); and by the House of Lords in *In re L (a Minor) (Police Investigation: Privilege)* [1997] AC 16, 24–5 (*per* Lord Jauncey) and *Three Rivers District Council and others v. Governor and Company of the Bank of England (No. 6)* [2005] 1 AC 610, HL (*Three Rivers No. 6*), para. 65 (*per* Lord Carswell) and paras. 50, 51 (*per* Lord Rodger).

4 See *Thanki* (ed.), *The Law of Privilege* (3rd edn.), para. 2.02.

5 See *Thanki*, paras. 1.09 to 1.12; Passmore, *Privilege* (4th edn.), paras. 3-002 to 3-006.

6 *Three Rivers No. 6*, para. 24 (*per* Lord Scott).

7 *Bursill v. Tanner* (1885) 16 QBD 1, 4; *Pascall v. Galinski* [1970] 1 QB 38; *R (Miller Gardner) v. Minshull St Crown Court* [2002] EWHC 3077 (Admin); *R (Howe) v. South Durham Magistrates Court* [2005] RTR 4. See, generally, A Pugh-Thomas, 'Who is your client?' (1997) SJ 141(2) 44.

8 *Ex Parte Campbell* (1869–70) LR 5 Ch App 703, 705. However, in this case James LJ made clear that the position may be different if the client's residence has been told to the lawyer as a matter of professional confidence. These *dicta* were applied in *Re Arnott, ex p Chief Official Receiver* (1888) 60 LT 109.

© Law Business Research 2021

retainer[9] will not generally be deemed to be confidential (or, accordingly, privileged). While a lawyer will usually owe his or her client enforceable duties of confidence,[10] for the purposes of litigation privilege, communications between a lawyer or client and a third party do not have to be 'confidential' in the sense that the third party is bound by equitable (or contractual) duties of confidence not to reveal the communication to anyone else.[11] In the context of litigation privilege, the requirement of confidentiality is therefore perhaps best put in terms of the communication or other document being 'not properly available for use'.[12]

36.2.2 Legal professional privilege as a substantive right

Legal professional privilege is not merely an exclusionary rule of evidence, but is also a substantive right, which is afforded overriding importance within English law.[13] The House of Lords and the Supreme Court have repeatedly emphasised its importance and its role in the administration of justice. It has been characterised as both 'a fundamental human right'[14] and 'a fundamental condition on which the administration of justice as a whole rests'.[15]

If it were simply a rule of evidence, a client could only prevent disclosure in legal proceedings. There would be no guarantee that the same material could be kept from the police or some other agency, such as a financial regulator or prosecuting authority, with the power to compel the production of documents or information. Hence, legal professional privilege can now generally be asserted in answer to any demand for documents by a public or other authority; it is not limited to a right that may be asserted only in the context of civil or criminal proceedings.

It is, however, a rule relating to immunity rather than admissibility,[16] since even improperly obtained privileged material may be admissible in evidence.[17]

---

9 *Levy v. Pope* (1829) M & M 410; *Gillard v. Bates* (1840) 6 M & W 547.

10 Confidentiality in this context is properly understood in the broader sense of information that the lawyer is not at liberty to disclose and may include information about a client that is in fact in the public domain: see decision of House of Lords in *Hilton v. BBE* [2005] 1 WLR 567, para. 34.

11 *ISTIL Group Inc v. Zahoor* [2003] 2 All ER 252, para. 60 (*per* Lawrence Collins J).

12 See *Bourns Inc v. Raychem Corp* [1999] 3 All ER 154, 167, 168, CA.

13 *R v. Derby Magistrates Court, ex p B* [1996] AC 487, 507, 508, HL; *General Mediterranean Holdings SA v. Patel* [2000] 1 WLR 272; *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 7.

14 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 7, HL (*per* Lord Hoffmann).

15 *R v. Derby Magistrates' Court, Ex p B* [1996] AC 487, 507 (*per* Lord Taylor CJ, with whom Lords Mustill and Lloyd agreed).

16 McE v. Prison Service of Northern Ireland [2009] 1 AC 908, para. 5, HL (per Lord Phillips).

17 *Calcraft v. Guest* [1898] 1 QB 759, CA; *R v. Tompkins* (1977) 67 Cr App R 181. The party to whom the privilege belongs might apply for an injunction to restrain its use: *Ashburton v. Pape* [1913] 2 Ch 469, CA; *Goddard v. Nationwide Building Society* [1987] QB 670, CA.

© Law Business Research 2021

The privilege is absolute and can only be overridden in very exceptional circumstances.[18] Furthermore, in accordance with the aphorism 'once privileged, always privileged',[19] once a client's privilege has attached to a document or other privileged exchange, the privilege will persist, subject only to waiver or other types of loss, for the client's benefit and that of successors in title for all time and in all circumstances.[20]

Rationale 36.2.3

The rationales underlying legal advice and litigation privilege are distinct:

- The interest protected by legal advice privilege is the public concern to ensure the availability of appropriate legal advice and assistance.[21] To this end, English law recognises the need to promote absolute candour between client and lawyer, by providing that exchanges between them will not subsequently be divulged.[22]
- Litigation privilege has often been regarded as an aspect of the right to a fair trial in England and in other common law jurisdictions.[23] The courts have emphasised that fairness requires a private and confidential sphere of preparation for litigation.[24] In a classic statement of this principle James LJ emphasised that 'as you have no right to see your adversary's brief, you have no right to see that which comes into existence merely as materials for

18 As Lord Scott stated in *Three Rivers No. 6* (para. 25): 'if a communication or document qualifies for legal professional privilege, the privilege is absolute. It cannot be overridden by some supposedly greater public interest. It can be waived by the person, the client, entitled to it, and it can be overridden by statute . . . but it is otherwise absolute. There is no balancing exercise that has to be carried out: see *B v. Auckland District Law Society* [2003] 2 AC 736, 756–59.' This was reiterated by the Court of Appeal in the recent case of *Victorygame Ltd v. Ahuja Investments Ltd* [2021] EWCA Civ 993. The Court added that it seemed likely that Lord Scott's reference to waiver in *Three Rivers No. 6* 'was shorthand for both waiver and estoppel', and that it 'must be possible' for a party to become estopped from claiming privilege, if the conduct or representation in question was clear and unequivocal and relied upon by the other party to their detriment: para. 54. (No such estoppel was made out in that case.)

19 For examples of its use, see *Calcraft v. Guest* [1898] 1 QB 759, 761, CA, and *Pearce v. Foster* (1885) 15 QBD 114, 119, CA.

20 See *Thanki*, paras. 1.68 to 1.74. See also *Addlesee v. Dentons Europe LLP* [2020] Ch 243.

21 See, generally, *Thanki*, paras. 1.17 to 1.22.

22 *Pearse v. Pearse* (1846) 1 De G & Sm 12, 28, 29 (*per* James Knight Bruce V-C) (cited with approval by Lord Carswell in *Three Rivers No. 6*, para. 112). See also *Pearce v. Foster* (1885) 15 QBD 114, 119 and 120 (*per* Sir Baliol Brett MR); *Re L* [1997] AC 16, 32 (*per* Lord Nicholls) (also cited with approval in *Three Rivers No. 6*, para. 112).

23 *Re Saxton* [1962] 1 WLR 968, 972 (*per* Lord Denning); *Baker v. Campbell* (1983) 49 ALR 385, 427 (*per* Brennan J).

24 *Three Rivers No. 6*, para. 52 (*per* Lord Rodger); *Robert Hitchins Ltd v. ICL* (CA, 10 Dec. 1996) (*per* Simon Brown LJ); *Sumitomo Corporation v. Credit Lyonnais Rouse Ltd* [2002] 1 WLR 479, para. 46, CA (*per* Jonathan Parker LJ).

© Law Business Research 2021

that brief'.[25] Litigation privilege has therefore been characterised by Lord Justice Steyn as an auxiliary principle buttressing the constitutional right of access to justice.[26] This rationale has been doubted, largely on the grounds that changes to English civil procedure (particularly the rules of pretrial disclosure) have introduced a culture of openness, which sits uneasily with any right to 'secrecy' in adversarial litigation.[27] However, litigation privilege remains justified by the need for a zone of privacy in the preparation for litigation[28] and remains firmly entrenched in English law as a consequence of decisions at appellate level, including the House of Lords.[29]

36.2.4 No adverse inference can be drawn where privilege is relied on

No adverse inferences may be drawn from the assertion by a person of a claim to legal professional privilege.[30] This is a principle that may sometimes be overlooked when an authority is seeking disclosure of privileged materials. But any responsible regulator or prosecuting authority must accept that it can neither require disclosure of privileged communications, nor rely on the regulated entity's refusal to provide it. As Lord Scott observed in *Three Rivers No. 6*, the existence of legal professional privilege means that 'cases may sometimes have to be decided in ignorance of relevant probative material'.[31]

Separately, however, there is some uncertainty as to whether UK prosecuting authorities can require privilege to be waived when entering into co-operation agreements with parties.[32] In *R v. George*,[33] a case against certain British Airways executives concerned with a cartel offence involving alleged collusion with Virgin Atlantic, this issue arose in circumstances where the relevant Virgin Atlantic executives had admitted the offences and were given immunity from prosecution by the Office of Fair Trading (OFT).[34] Under the OFT's leniency and immunity guidelines, these executives were expected to assume an obligation of continuous and complete co-operation with the OFT's investigation and any subsequent proceedings. Justice Owen considered that it

25 *Anderson v. Bank of British Columbia* (1876) 2 Ch D 644, 656. See to similar effect *Waugh v. British Railways Board* [1980] AC 521, 531 (*per* Lord Wilberforce).

26 *Oxfordshire CC v. M* [1994] Fam 151, 163, CA.

27 See *Secretary of State for Trade & Industry v. Baker* [1998] Ch 356, 371 (*per* Sir Richard Scott V-C); *Visx Inc v. Nidex* [1999] FSR 91; *Three Rivers No. 6*, paras. 29 (*per* Lord Scott) and 53 (*per* Lord Rodger).

28 See *Thanki*, para. 3.153; *Passmore*, paras. 3-010 to 3-033.

29 See *Thanki*, para. 1.25.

30 *Wentworth v. Lloyd* (1864) 10 HLC 589; *Sayers v. Clarke Walker* [2002] EWHC Ch 60, para. 52.

31 *Three Rivers No. 6*, para. 34.

32 See, generally, *Passmore*, paras. 1-083 to 1-093.

33 Unreported, 7 Dec. 2009.

34 The OFT has now been superseded, along with the Competition Commission, by the Competition and Markets Authority (CMA), though regulation of consumer credit passed to the Financial Conduct Authority (FCA).

© Law Business Research 2021

would be reasonable for the OFT to press for disclosure of privileged material in the hands of the Virgin Atlantic executives, as part of the OFT's duty to obtain material held by a third party that might be capable of undermining the prosecution case, on the basis that the Virgin Atlantic executives were under a duty to give continuous and complete co-operation as a condition of leniency or immunity; and, failing a satisfactory response, it would be reasonable for the OFT to invoke its power to revoke the leniency agreements.[35] By contrast, in *R v. Daniels*,[36] in which a co-defendant to a murder charge had entered into an agreement pursuant to section 73 of the Serious Organised Crime and Police Act 2005 (SOCPA) under which he agreed to give assistance to the authorities, the Court of Appeal did not express a view as to whether a requirement to waive privilege could lawfully be included in a SOCPA agreement and indicated (without deciding) that, if so, an express condition would be required. The ability of a prosecuting authority to require waiver of privilege, and the circumstances in which it will be taken to have done so, therefore remains in some doubt and would appear to vary depending on the particular rules and guidelines applicable to the prosecuting authority.

Since the decision in *R v. George*, the OFT guidance 'Applications for leniency and no-action in cartel cases' (the 2013 Leniency Guidance), now adopted by the Competition and Markets Authority (CMA), has changed and no longer requires waiver of privilege as an element of co-operation. However, the CMA does not rule out enquiring as to whether a leniency applicant may be prepared to waive privilege over certain material during the course of a possible criminal cartel prosecution, although making it clear that any refusal to waive privilege will not have any adverse consequences for the leniency application and that granting such a waiver would not yield any advantage to the leniency applicant. The CMA (like the Serious Fraud Office (SFO)) will, unless the position is uncontroversial, instruct independent counsel to provide an opinion on whether the relevant information is privileged and will require disclosure of information not found to be privileged.[37]

It is also clear that a party's willingness to waive privilege may be taken into account by the SFO in considering whether to enter into a deferred prosecution agreement (DPA) and is a relevant factor to be taken into account by a court when considering, pursuant to section 45 and Schedule 17 of the Crime and Courts Act 2013, whether to approve a DPA.[38] The SFO's Corporate Co-operation Guidance states: 'An organisation that does not waive privilege

35 The case against the BA executives ultimately collapsed following the discovery of thousands of prosecution e-disclosure documents that had neither been disclosed to BA nor reviewed by the OFT.

36 [2010] EWCA Crim 2740.

37 2013 Leniency Guidance, paras. 3.15 to 3.23.

38 *Serious Fraud Office v. Rolls-Royce plc* [2017] Lloyd's Rep FC 249, paras. 19 to 21, 35 to 39, 121; *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 117.

© Law Business Research 2021

and provide witness accounts does not attain the corresponding factor against prosecution that is found in the DPA Code . . . but will not be penalised by the SFO'.[39]

36.2.5 Privilege belongs to the client

Privilege belongs to the client and not to the lawyer or agent.[40] Only the client can invoke the privilege.[41] It is not open to a lawyer or other agent to do so, unless acting on behalf of the client, and the lawyer or agent cannot invoke the privilege if the client has waived it.[42] In the case of litigation privilege, a third party with whom a lawyer or client has communicated for the purposes of adversarial proceedings may not assert the privilege of the party to the actual or prospective litigation.[43]

36.3 Legal advice privilege

The scope of legal advice privilege was the subject of authoritative reconsideration by the House of Lords in *Three Rivers No. 6*. Lord Rodger defined the privilege (at paragraph 50) as extending to:

> *[A]ll communications made in confidence between solicitors and their clients for the purpose of giving or obtaining legal advice even at a stage where litigation is not in contemplation. It does not matter whether the communication*

39 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/corporate-co-operation-guidance/.

40 *R v. Derby Magistrates' Court, ex p B* [1996] AC 487, 504, 505, HL.

41 Although the lawyer is under a professional obligation to assert the privilege on behalf of his or her client unless it has been waived: *R v. Central Criminal Court, ex p Francis & Francis* [1989] AC 346, 383, HL; *Bolkiah v. KPMG* [1999] 2 AC 222, 235, 236, HL; *Nationwide Building Society v. Various Solicitors* [1999] PNLR 52, 69. The court may also intervene to prevent a third party or even the client's lawyer making disclosure in breach of the client's privilege: *Harmony Shipping v. Saudi Europe Line* [1979] 1 WLR 1380, 1384, 1385, CA. In *A v. B and Financial Reporting Council* [2020] 1 WLR 3989, the court considered the position where a regulator issues a statutory notice requiring a regulated entity (B) to produce documents that the client (A) of that entity asserts are subject to A's privilege but that B does not consider to be privileged. It was held, contrary to the submissions of A, that B is not obliged to assert the privilege of A, and to withhold the documents from the regulator, without regard to the strength of A's claim to privilege, but must assess the quality of the claim to privilege for itself. Of course, if B has any doubt, it is very likely that it will seek a determination from the court, to avoid the risk of incurring liability to A. If A is aware that B is considering providing documents to its regulator that A considers to be privileged, A can also apply for an injunction to prevent disclosure. In either scenario, the question of whether the documents are actually privileged is to be decided by the court.

42 *Re International Power Industries* [1985] BCLC 128; *R v. Peterborough Justices, ex p Hicks* [1977] 1 WLR 1371; *Nationwide Building Society v. Various Solicitors (No. 2) The Times*, 1 May 1988.

43 *Lee v. SW Thames Health Authority* [1985] 1 WLR 845, CA; *Schneider v. Leigh* [1955] 2 QB 195.

© Law Business Research 2021

> *is directly between the client and his legal advisor or is made through an intermediate agent of either.*

The requirements thereby identified can be summarised as follows: (1) a communication, whether written or oral, (2) between a client and a lawyer (or an intermediate agent of either), (3) made in confidence[44] (4) for the dominant purpose of giving or obtaining legal advice.[45]

Communication 36.3.1

The basic concept of communication is self-explanatory. However, privilege does not arise upon the exchange of pre-existing and previously unprivileged documents: the document's existence must be attributable to the intention to communicate.[46] The scope of the privilege is, however, broader than references merely to 'communications' might seem to indicate. In addition to communications, the following documents will also (if the remaining requirements are satisfied) fall within the privilege:

- a document intended to be a communication between client and lawyer, which was never communicated;[47]
- documents or parts of documents that evidence the substance of lawyer–client communications.[48] This would include, for example, a written record of an oral communication or a document disseminating the contents or substance of legal advice within[49] or even beyond[50] the corporation receiving the advice; and
- the lawyer's working papers, including drafts, attendance notes and memoranda.[51]

---

44 This requirement has been considered in Section 36.2.1.

45 The requirement that the purpose of giving or obtaining legal advice must be the dominant purpose was confirmed in *Civil Aviation Authority v. R (Jet2.Com)* [2020] 2 WLR 1215.

46 *Pearce v. Foster* (1885) 15 QBD 114, 118–19, CA; *R v. Peterborough Justices, ex p Hicks* [1977] 1 WLR 1371, 1374; *Ventouris v. Mountain* [1991] 1 WLR 607, 616, CA (*per* Bingham LJ). This is so even if the pre-existing unprivileged document is attached to a privileged email (*Financial Reporting Council Limited v. Sports Direct International* [2020] 2 WLR 1256).

47 *Three Rivers No. 6*, para. 21.

48 *Three Rivers District Council and others v. Governor and Company of the Bank of England (No. 5)* [2003] QB 1556 (CA) (*Three Rivers No. 5*), paras. 19, 26.

49 *Bank of Nova Scotia v. Hellenic Mutual War Risks Association (Bermuda) Ltd (The Good Luck)* [1992] 2 Lloyd's Rep, 540.

50 *USP Strategies Plc v. London General Holdings Ltd* [2004] EWHC (Ch) 373.

51 *Greenough v. Gaskell* (1833) 1 M&K, 98, 101, 102 (entries made by the lawyer in his accounts held to be privileged); *Ainsworth v. Wilding* [1900] 2 Ch, 315, 323 (*per* Stirling J) (notes or memoranda made by a lawyer are placed on the same footing as communications between lawyer and client); *Balabel v. Air India* [1988] Ch, 317, 323 (*per* Taylor LJ); *Three Rivers No. 5*, para. 30.

© Law Business Research 2021

36.3.2 Between a client and lawyer

36.3.2.1 Lawyer

The scope of the term 'lawyer' for the purposes of legal advice privilege (and legal professional privilege more generally) is broad rather than formalistic, but not without limits. In *R (Prudential PLC) v. Special Commissioner of Income Tax*, the Supreme Court confirmed that legal professional privilege is applicable only to 'communications in connection with advice given by members of the legal profession, which includes members of the Bar, the Law Society, and the Chartered Institute of Legal Executives (CILEX) (and, by extension, foreign lawyers)'.[52] The privilege extends to their non-qualified employees including secretaries,[53] clerks, trainee solicitors, pupils or paralegals acting under the direction of a lawyer.[54] For the avoidance of doubt, under English law[55] no distinction is made between in-house lawyers and lawyers in independent practice.[56] However, that an individual happens to be a 'lawyer' in the sense required above will not suffice; in each case the relevant question is whether he or she is consulted in that professional capacity.[57] The lawyer must also be subject to the control of the professional body and the governing rules of practice; in other words, the lawyer must have a current practising certificate. Therefore, a qualified solicitor who has been struck off the roll is not a lawyer for the purposes of

52 *R (Prudential PLC) v. Special Commissioner of Income Tax* [2013] 2 AC 185, para. 29, SC. On communications with foreign lawyers, see *Thanki*, para. 1.52.

53 *Descoteaux v. Mierzwinski* (1982) 141 DLR (3d) 590, 603.

54 *Taylor v. Forster* (1825) 2 C&P 195; *Wheeler v. Le Marchant* (1881) 17 Ch D 675, 682, CA.

55 This is subject to one narrow exception: the European Court of Justice has held that, as a matter of European Community law, parties to investigations into alleged breaches of Articles 81 (now 101) and 82 (now 102) of the Treaty of Rome cannot claim legal professional privilege for internal communications with employees, even if the employee is acting as an in-house lawyer: *Akzo Nobel Chemicals Ltd v. European Commission*, Case C550/07 P.

56 *Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs* (No. 2) [1972] 2 QB, 102, 129 (*per* Lord Denning MR) CA. This conclusion was not challenged on appeal: *Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs (No. 2)* [1974] AC, 405, 430 and 431, HL.

57 *Minter v. Priest* [1930] AC 558, 581 (*per* Lord Atkin). In *Ms A v. UBS AG*, Employment Tribunal Case Number 2200832/2019 (1 Nov. 2019, published Apr. 2021), a report prepared by a partner at Freshfields Bruckhaus Deringer LLP into UBS's handling of a rape allegation made by an employee was found not to be privileged because the evidence indicated that the partner had been selected to conduct the review not because she was a lawyer or because she worked for Freshfields (indeed the person at UBS who appointed her had said he had not known she worked for the firm) but because of her other relevant skills and experiences: paras. 37, 39. Nor was the Freshfields partner instructed or asked to give legal advice: para. 38.

© Law Business Research 2021

legal professional privilege,[58] unless the client in good faith does not know that the solicitor has been struck off.[59]

Subject to certain specific statutory exceptions,[60] communications with other professionals – including, for example, patent and trade mark attorneys – will not attract legal advice privilege at common law, even where they are giving advice on strictly legal matters.[61]

Legal advice privilege will apply to advice received from foreign lawyers, including in-house foreign lawyers.[62] The court will not enquire into whether or how the foreign lawyer is regulated, or what rules or practices apply to that lawyer under the local law, as long as the foreign lawyer is acting in the capacity of a lawyer.[63] The privilege covers advice given by foreign lawyers on English law[64] as well as foreign law.[65]

Client 36.3.2.2

The concept of the 'client' in the context of corporations was the subject of appellate consideration by the Court of Appeal in *Three Rivers No. 5* and has recently been the subject of further consideration by the Court of Appeal in

58 *Dadourian Group International and others v. Simms and others* [2008] EWHC 1784 (Ch), paras. 119 to 128. See also *Waterford v. Commonwealth of Australia* (1987) 163 CLR, 54, 81, 82 (*per* Deane J).

59 *Dadourian Group International and others v. Simms and others* [2008] EWHC 1784 (Ch), para. 127. The burden is on the client to show that he or she continued to believe that the solicitor held a practising certificate at the time.

60 For example: patent attorneys (Copyright, Designs and Patents Act 1988, s.280); trademark attorneys (Copyright, Designs and Patents Act 1988, s.284); licensed conveyancers (Administration of Justice Act 1985, s.33); authorised advocates and litigators (Courts and Legal Services Act 1990, s.63). It is clear that patent and trademark attorneys do not attract legal professional privilege at common law: *Dormeuil Trade Mark* [1983] RPC 131; *Wilden Pump Engineering Co v. Fusfield* [1985] FSR 159, CA; *R (Prudential plc) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC 185, para. 68.

61 *R (Prudential Plc) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC, 185. See R Pattenden, *The Law of Professional–Client Confidentiality* (2003), para. 16.42, for a comprehensive list of other professions to which privilege has been expressly denied, including doctors, accountants, priests, bankers, auditors and journalists.

62 See *R (Prudential PLC) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC 185, paras. 45, 73; *PJSC Tatneft v. Bogolyubov & Ors* [2020] EWHC 2437 (Comm), para. 57.

63 In *PJSC Tatneft v. Bogolyubov & Ors* [2020] EWHC 2437 (Comm), as a matter of English law (as the *lex fori*) legal advice privilege applied to communications with the in-house lawyers of the claimant, a Russian company, even though it was said that in Russia, in-house lawyers are not members of the Russian bar (advocates) and the Russian concept equivalent to legal professional privilege (advocate's secrecy) does not apply to them.

64 *International Business Machines Corp v. Phoenix International (Computers) Ltd* [1995] 1 All ER 413, 429; *Ritz Hotel Ltd v. Charles of the Ritz Ltd (No. 4)* (1987) 14 NSWLR 100, 100–02.

65 *Bunbury v. Bunbury (1839) 2 Beav 173; Macfarlan v. Rolt* (1872) LR 14 Eq 580.

© Law Business Research 2021

The Director of the Serious Fraud Office v. ENRC[66] and *R (Jet2.com Limited) v. Civil Aviation Authority*[67] (discussed later in this section). The true *ratio* of *Three Rivers No. 5* has been the subject of controversy. In previous editions of this work, it was said that it appeared that the 'client' would not necessarily be the corporation itself, or its employees *per se*, but only those within the corporation who were authorised to communicate with the lawyer and receive his or her advice.[68] This was the interpretation of *Three Rivers No. 5* adopted by the Singapore Court of Appeal in *Skandinaviska Enskilda Banken v. Asia Pacific Breweries*. The court in that case commented that the principle is that 'if an employee is not authorised to communicate with the company's solicitors for the purpose of obtaining legal advice, then that communication is not protected by legal advice privilege'. It went on to state that authorisation need not be express but may be implied.[69]

However, the concept of the 'client' was interpreted more restrictively in two first-instance decisions of the English High Court.[70] In *The RBS Rights Issue Litigation*,[71] Justice Hildyard held that notes of witness interviews prepared by RBS's lawyers were not subject to legal advice privilege (although the interviewees were authorised by RBS to communicate with the lawyers), and neither were the notes subject to legal advice privilege on the basis that they comprised lawyers' working papers. In Hildyard J's view, the Court of Appeal in *Three Rivers No. 5* established a general principle that 'the client' for the purposes of a lawyer–client communication subject to legal advice privilege must be someone who is authorised to seek and receive legal advice. The approach in *The RBS Rights Issue Litigation* was followed by Mrs Justice Andrews in the first-instance decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation*,[72] where once again the privileged status of interview notes produced by the lawyers during the course of an internal investigation was in issue. Andrews J held that legal advice privilege attaches only to 'communications between the lawyer and those individuals

66 [2019] 1 WLR 791.

67 [2020] 2 WLR 1215.

68 See *Three Rivers No. 5*, para. 31 (*per* Longmore LJ, giving judgment of Court of Appeal).

69 *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v. Asia Pacific Breweries (Singapore) Pte Ltd* [2007] 2 SLR 367, para. 42.

70 A similar approach was also taken by Chief Master Marsh in *Astex v. Astrazeneca* [2016] EWHC 2759 (Ch) and by the Divisional Court in *R(AL) v. Serious Fraud Office* [2018] EWHC 856 (Admin) (although the reasoning on this issue in that case is somewhat confused, perhaps because – on the unusual facts of the case – no party was positively asserting that privilege applied to the interview notes in question).

71 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

72 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205.

© Law Business Research 2021

who are authorised to obtain legal advice on that entity's behalf'.[73] By 'authorised' Andrews J meant being specifically 'tasked' by the corporation to obtain legal advice, a qualification not found in the judgment of the Singapore Court of Appeal in the *Skandinaviska* case referred to above. That interviewees were authorised to communicate with the lawyers to provide them with information or relevant facts in order for the lawyers to give advice, did not make those communications privileged. Andrews J also agreed with Hildyard J that lawyers' notes of interviews with witnesses would not be privileged on the ground of being lawyers' working papers, unless the notes would betray the tenor of the legal advice.

The issue came before the Court of Appeal in *The Director of the Serious Fraud Office v. ENRC*.[74] The Court analysed the decision in *Three Rivers No. 5* and concluded as follows:

> *We can fully accept that the Court of Appeal could have decided* Three Rivers (No. 5) *on the simple basis that Freshfields' client was the BIU*[75] *(not the Bank), and the documents had been prepared by the Bank (not the BIU), so that the position of the particular Bank employee who had prepared them was irrelevant to the question of legal advice privilege. We do not, however, think that, fairly read, that was the Court of Appeal's reasoning. . . . it seems to us that Longmore LJ reasoned that, because agents and employees, on authority, stood in the same position in relation to legal professional privilege, once it was established that only communications between the lawyer and the client, and not between the lawyer and an agent of the client, could attract legal advice privilege, communications between a lawyer and an employee of the client (other than employees specifically tasked with seeking and receiving legal advice) could also not be privileged. As we have said, we are not sure that it is necessary for us to determine whether this reasoning was the* ratio decidendi, *but if that did have to be decided, we would hold that it was.*[76]

As to whether *Three Rivers No. 5* was correctly decided on this point, the Court of Appeal in *ENRC* held[77] that this is a question which can only be determined

73 ibid., para. 70. Andrews J acknowledged that, in the context of a company, the person giving the instructions to the lawyers may not necessarily be the same as the person or persons who want to receive the advice. Accordingly, there could be instances where particular individuals or groups are authorised to instruct the lawyers, while others individuals are authorised to receive the advice, typically a company's board of directors (see ibid., para. 84).

74 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791.

75 The BIU was a unit that had been set up within the Bank of England (the Bank) for dealing with matters regarding the inquiry in relation to which the lawyers, Freshfields, had been retained by the Bank.

76 [2019] 1 WLR 791, para. 81.

77 ibid., para. 124.

© Law Business Research 2021

by the Supreme Court. Nevertheless, the Court expressed the view that there was 'much force' in submissions made on behalf of ENRC and The Law Society (intervening in the appeal) that, if *Three Rivers No. 5* did indeed decide that the definition of 'client' should be restrictively interpreted as it was in *The RBS Rights Issue Litigation*, then it was wrongly decided. The Court referred to the policy justification for legal advice privilege, that there is a public interest in a client being able to place all the facts before the legal adviser without fear that they may afterwards be disclosed and used to the client's prejudice, and to the fact that large corporations need, as much as small corporations and individuals, to seek and obtain legal advice without fear of intrusion. The Court acknowledged that, in the modern world, legal advice is often sought by large national and multinational companies where the information on which legal advice is sought is unlikely to be in the hands of the main board or those it appoints to seek and receive legal advice; therefore:

> *If a multi-national corporation cannot ask its lawyers to obtain the information it needs to advise that corporation from the corporation's employees with relevant first-hand knowledge under the protection of legal advice privilege, that corporation will be in a less advantageous position than a smaller entity seeking such advice. In our view, at least, whatever the rule is, it should be equally applicable to all clients, whatever their size or reach.*[78]

The Court also referred to English law being out of step on this issue with the international common law and remarked on the undesirability of such inconsistency. The Court concluded that:

> *If, therefore, it had been open to us to depart from* Three Rivers (No. 5), *we would have been in favour of doing so. For the reasons we have given, however, we do not think that it is open to us, so it is a matter that will have to be considered again by the Supreme Court in this or an appropriate future case.*[79]

The Court of Appeal in *R (Jet2.com Limited) v. Civil Aviation Authority* agreed with those sentiments, Lord Justice Hickinbottom holding that he would have been disinclined to follow *Three Rivers 5* if that had been in the court's power.[80] If the issue finally reaches the Supreme Court, there is every chance that the restrictive interpretation of 'client' will be reconsidered but, until then, the law should be taken to be as stated by the Court of Appeal in *ENRC*.

The implications of a restrictive interpretation of 'client' in a corporate context are well rehearsed. This approach is likely to exclude the vast majority of employees within the company. A corporate entity that wishes to obtain

78 ibid., para. 127.

79 ibid., para. 130.

80 [2020] 2 WLR 1215, para. 57.

© Law Business Research 2021

legal advice and that needs to carry out a fact-finding investigation within the organisation to obtain the necessary information for its lawyers will not, while these decisions on the proper interpretation and application of *Three Rivers No. 5* remain good law, be able to claim legal advice privilege over documents created pursuant to that fact-finding investigation (except, it seems, to the extent that the facts are known to, and obtained by the lawyers from, individuals who also happen to be authorised to seek and receive legal advice). While the rationale of legal advice privilege is, as explained in Section 36.2.3, to enable a client to provide full and frank instructions to its lawyer to enable the lawyer to provide sensible advice, it appears that (pending any clarification from the Supreme Court) a corporate client will be severely restricted in the extent to which it can gather information for its lawyer in order for the lawyer to give advice without its communications being disclosable in subsequent proceedings. It makes no difference whether information is obtained from employees by other employees of the company or by the lawyers directly.

In this regard, and as recognised by the Court of Appeal in *ENRC*, English law is also at odds with other common law jurisdictions. The Hong Kong Court of Appeal in *CITIC Pacific v. Secretary of State for Justice*[81] recognised that a narrow definition of client was incompatible with the rationale for legal advice privilege as explained by the House of Lords in *Three Rivers No. 6*. The decisions in *The RBS Rights Issue Litigation* and, at first instance, in *ENRC* also seem to be doubtful in relation to the lawyers' working papers doctrine. Notes of witness interviews that are prepared by lawyers, provided they are not verbatim transcripts, are types of document that should typically qualify as 'lawyers working papers', in line with the decision in *Balabel v. Air India*.[82] This was the subject of argument before the Court of Appeal in *ENRC*. However, the Court declined to decide this issue because, in light of its findings on litigation privilege, it did not strictly arise and moreover the Court considered that it would be preferable for the matter to be addressed by the Supreme Court in the context of any future consideration of legal advice privilege.[83]

81 [2012] 2 HKLRD 701.

82 In this regard there must be some doubt as to whether the court was correct in *The RBS Rights Issue Litigation* and in *ENRC* – at first instance – in stating that to qualify as lawyers' working papers, documents must betray the trend of legal advice. That is not a requirement specified in *Balabel* (in which the Court of Appeal was considering a claim to privilege in respect of both communications between client and lawyer and lawyers' working papers) nor is it required in *Three Rivers No. 5* itself. In specifying that requirement Hildyard J in *The RBS Rights Issue Litigation* and Andrews J in *ENRC* relied on observations made in a different context, namely where a solicitor copies or assembles a collection of documents, and the issue is whether that selection can be said to be privileged (see *Lyell v. Kennedy (No. 3)* (1884) 27 Ch D 1; subsequently commented on by Bingham LJ in *Ventouris v. Mountain* [1991] 1 WLR 607).

83 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, paras. 141, 142.

© Law Business Research 2021

Communication need not in all cases be direct, but may occur through an agent of the client or the lawyer. A distinction needs to be made between an agent for the purposes of communication, that is to say a mere conduit between the client and the lawyer, such as an interpreter (where intellectual input by the agent will risk destroying the privilege[84]) and an agent for the purposes of seeking and obtaining the advice (where it will not). Communications between 'the various legal advisers of the client' with a view to the client obtaining legal advice or assistance will generally be privileged.[85]

36.3.3 For the dominant purpose of giving or obtaining legal advice or assistance

In *Three Rivers No. 6*, the House of Lords unanimously[86] adopted a statement by Lord Justice Taylor in *Balabel v. Air India*[87] that:

> *[L]egal advice is not confined to telling the client the law; it must include advice as to what should prudently and sensibly be done in the relevant legal context.*

In most cases the relevant 'legal context' will be obvious. Where there is room for doubt, Lord Scott suggested[88] that the court should consider whether:

- the advice sought from the lawyer relates to the rights, liabilities, obligations or remedies of the client either under private or public law; and
- the communication falls within the policy underlying the justification for legal advice privilege. In short, 'is the occasion on which the communication takes place and is the purpose for which it takes place such as to make it reasonable to expect the privilege to apply?'

Notwithstanding the first limb of Lord Scott's test, it appears that the 'legal context' is not actually confined to advice concerning the client's legal rights and liabilities. The relevant communications in *Three Rivers No. 6* involved presentational advice as to how the client (the Bank of England) could best put material before an inquiry, established by the Chancellor of the Exchequer and the Governor of the Bank, which was scrutinising the discharge of the Bank's public duties. The House of Lords held that legal advice privilege plainly applied. Lord Rodger emphasised[89] that privilege would similarly have applied 'to presentational advice sought from lawyers by any individual or company who believed himself, herself or itself to be at risk of criticism by an inquiry', emphasising that the 'defence of personal reputation and integrity is at least as

84 See *Thanki*, para. 2.77.

85 *Trade Practices Commission v. Sterling* (1979) 36 FLR 244, para. 4.

86 *Three Rivers No. 6*, paras. 38, 59, 62, 111, 122.

87 [1988] Ch. 317, 330, CA.

88 *Three Rivers No. 6*, para. 38.

89 ibid., para. 44.

© Law Business Research 2021

important to many individuals and companies as the pursuit or defence of legal rights whether under private law or public law'.

In substance, the test is whether the lawyer is reasonably being consulted because of his or her legal skills. This is reflected in the emphasis placed by the House of Lords on whether the lawyer is being consulted '*qua* lawyer',[90] or is being asked to 'put on legal spectacles'[91] and whether the lawyer is being required to exercise 'special professional knowledge and skills'.[92] The concept of a 'legal context' is therefore very broad, although it remains the case that a lawyer might perform a non-legal function (for example, a secretarial function in editing meeting minutes,[93] or where a lawyer has been appointed to conduct a review because of relevant non-legal skills and experiences and without regard to the fact they are a lawyer[94]) with the result that privilege may not attach.

Once a 'legal context' is established, the question is whether the relevant communication falls within it. The clearest definition of the ambit of legal advice in *Three Rivers No. 6* was that provided by Lord Carswell (with whom all the Law Lords expressly agreed[95]), in the following passage:

> *[A]ll communications between a solicitor and his client relating to a transaction in which the solicitor has been instructed for the purpose of obtaining legal advice will be privileged, notwithstanding that they do not contain advice on matters of law or construction, provided that they are directly related to the performance by the solicitor of his professional duty as legal adviser of his client.*[96]

This passage can be regarded as an authoritative statement of the modern law. The House of Lords expressly rejected any requirement that the communication must itself contain 'legal advice', in any strict sense of that phrase. *Three Rivers No. 6* therefore both preserves and consolidates a line of authority that supports the attachment of privilege to documents that, while they do not

90 ibid., para. 58 (*per* Lord Rodger).

91 ibid., para. 60 (*per* Lord Rodger).

92 ibid., para. 62 (*per* Baroness Hale).

93 *A v. B and Financial Reporting Council Ltd* [2020] EWHC 1492 (Ch), para. 11. It was further held in that case that the party asserting privilege will still need to identify, either directly or by inference, a statement of the advice or communication that is said to be privileged. Such an inference will be drawn only if it is obvious. The involvement of a lawyer in the production of a document, or the mere fact that a document is headed 'privileged and confidential', will not in itself constitute a sufficient basis to infer that the document records legal advice (or advice as to what should prudently and sensibly be done in a legal context): see at paras. 11–14 and 24–25.

94 *Ms A v. UBS AG*, Employment Tribunal Case Number 2200832/2019 (1 Nov. 2019, published Apr. 2021): see supra note 57.

95 ibid., paras. 45, 49, 61, 119.

96 ibid., para. 111.

© Law Business Research 2021

contain legal advice, nevertheless form part of the 'continuum of communications' made for that broad purpose.

The law as stated above was given effect in the regulatory investigations context in the case of *Property Alliance Group v. RBS*.[97] In that case, RBS claimed privilege over documents prepared by its solicitors for the RBS Executive Steering Group (ESG), which had been established by RBS to oversee its response to various regulatory and criminal investigations into manipulation of LIBOR and other rates in the United Kingdom, United States and elsewhere. The claimant, Property Alliance Group (PAG), challenged RBS's claim to privilege over these documents, contending that the role of RBS's solicitors was not confined to the provision of legal advice but extended to the performance of administrative functions (for example, acting as the secretariat for the ESG and attending its meetings) for which privilege could not be claimed. Having inspected the disputed documents, Justice Snowden was 'entirely satisfied' that RBS's solicitors had been engaged in a relevant legal context. He remarked that:

> *RBS was facing Regulatory Investigations in a number of jurisdictions that could have had (and did have) the consequence that RBS was subjected to very large regulatory penalties and consequent private actions for very significant sums of money. Dealing with, and co-ordinating the communications and responses to such regulators was a serious and complex matter upon which RBS naturally wished to have the advice and assistance of specialist lawyers. Clifford Chance were engaged to provide such advice and assistance, and (to use Lord Scott's words), that advice and assistance undoubtedly related to the rights, liabilities and obligations of RBS, and the remedies that might be granted against it either under private law or under public law.*
>
> *I am also entirely satisfied that, in the words of Taylor LJ in* [Balabel] *the two types of ESG High Level Documents* [i.e. tabular memoranda informing and updating the ESG on the progress, status and issues arising in the regulatory investigations, and confidential notes or summaries drafted by Clifford Chance concerning the discussions between the ESG and its legal advisers at the ESG meetings] *form part of 'a continuum of communication and meetings' between Clifford Chance and RBS, the object of which was the giving of legal advice as and when appropriate.*[98]

Snowden J also rejected an argument made by PAG that the ESG documents should be only partly redacted, so that summaries of factual information would not be withheld from inspection, finding that such an approach would be

97 [2016] 1 WLR 992. See also *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205, para. 184.

98 *Property Alliance Group v. RBS* [2016] 1 WLR 992, paras. 27, 28.

© Law Business Research 2021

inconsistent with the *dicta* of Taylor LJ in *Balabel*.[99] While, depending on the facts, a court might not uphold a claim to privilege in respect of the minutes of a business meeting simply because the minutes were taken by a lawyer who was present and subsequently sent them to the client, that would be because the court would have taken the view that the lawyer was not being asked *qua* lawyer to provide legal advice.

As to the public policy implications of his judgment, Snowden J noted (at paragraph 45) that there is a clear public interest in regulatory investigations being conducted efficiently and in accordance with law and that the public interest will be advanced if regulators can deal with experienced lawyers who can accurately advise their clients how to respond and co-operate. Such lawyers must be able to give the client candid factual briefings as well as legal advice, secure in the knowledge that any such communications and any record of their discussions and the decisions taken will not subsequently be disclosed without the client's consent.

There has been doubt for some time as to whether, to attract legal advice privilege, a communication must be made with the dominant purpose of seeking or giving legal advice. This question was considered by the Court of Appeal in *R (Jet2.com) v. Civil Aviation Authority,* which concluded that, for legal advice privilege to apply to a particular communication or document, the proponent of the privilege must show that the dominant purpose of that communication or document was to obtain or give legal advice.[100] The Court of Appeal confirmed that the general instructions to, and role of, the relevant lawyer make 'a good starting point' but found that this does not determine the different question as to whether a specific document passing between client and lawyer is subject to legal advice privilege. Even if the dominant purpose of a lawyer's retainer (or his or her 'dominant role') relates to giving legal advice, that is not conclusive of whether legal advice privilege applies to a particular communication between lawyer and client. However, where the brief or role is *qua* lawyer, because 'legal advice' includes advice on the application of the law and the consideration of particular circumstances from a legal point of view, and because a broad approach is also taken to 'continuum of communications', most communications to and from the client are likely to be sent in a legal context and are likely to be privileged. It was noted that the court is unlikely to be persuaded by fine arguments as to whether a particular document or communication does fall outside legal advice, particularly as the legal and non-legal might be so intermingled that distinguishing the two and severance are for practical purposes impossible. In those circumstances, it can be properly said that the dominant purpose of the document as a whole is giving or seeking legal advice.

Notwithstanding this gloss, the articulation of a dominant purpose test for legal advice privilege is somewhat surprising given that the Court of Appeal in

99 *Balabel v. Air India* [1988] Ch 317, 330F.

100 [2020] 2 WLR 1215, para. 96.

© Law Business Research 2021

ENRC had rejected the argument. It is also hard to see how it is consistent with the 'relevant legal context' test set down by the House of Lords in *Three Rivers No. 6*. That said, it remains the law for the time being. While the dominant purpose requirement is unlikely to be an issue for many lawyer–client communications, it may be highly significant where multi-addressee communications are involved, as discussed in the section below.

36.3.4 Communications with multiple addressees

A difficult question that frequently arises in practice, particularly where in-house lawyers are involved, and which was addressed in *Jet2.com*, is how to determine the privileged status of communications (typically emails) to which a number of people are party, only one of whom is a lawyer. *Jet2.com* involved a challenge to the decision of the Civil Aviation Authority (CAA) to publish a press release about Jet2.com's refusal to participate in a new alternative dispute resolution scheme proposed for the aviation industry and the CAA's decision to publish correspondence between it and Jet2.com about that press release. In Jet2.com's application for disclosure of, *inter alia*, internal documents at the CAA relating to the drafting of the letter it had written to Jet2.com in response to its complaint, issues arose as to the application of legal advice privilege as a result of the involvement of in-house lawyers in the discussion and drafting of the letter.

The Court of Appeal held that the following approach should be adopted in respect of multi-addressee emails (i.e., emails exchanged between the client and a mixture of lawyers and non-lawyers):[101]

- In respect of a single, multi-addressee email sent simultaneously to various individuals for their advice or comments, including a lawyer for his or her input, the purpose of the communication must be identified. In this exercise, the wide scope of 'legal advice' (including the giving of advice in a commercial context through a lawyer's eyes) and the concept of 'continuum of communications' (as discussed above) must be taken fully into account.
- The response from the lawyer, if it contains legal advice, will almost certainly be privileged, even if it is copied to more than one addressee. Again, while the dominant purpose test applies, given the wide scope of 'legal advice' and 'continuum of communications', the court will be extremely reluctant to engage in the exercise of determining whether, in respect of a specific document or communication, the dominant purpose was the provision of legal (rather than non-legal) advice.
- In respect of the debate as to whether multi-addressee communications should be considered as separate bilateral communications between the sender and each recipient, or whether they should be considered as a whole, the Court preferred the former view. Where the purpose of the sender is simultaneously to obtain from various individuals both legal advice and

101 ibid., para. 100.

© Law Business Research 2021

non-legal advice or input, the Court considered it difficult to see why the form of the request (in a multi-addressee email rather than in separate emails) in itself should be relevant to whether the communications to the non-lawyers should be privileged (although the Court recognised that the form of the communication may in some cases reveal its true purpose).

- There is some benefit in taking the approach of considering whether, if the email were sent to the lawyer alone, it would have been privileged. If no, then the question of whether any of the other emails are privileged hardly arises. If yes, then the question arises as to whether any of the emails to the non-lawyers are privileged, because (for example) the dominant purpose of the email is to obtain instructions or disseminate legal advice.
- However, whether considered as a single communication or separate communications to each recipient, and while there may perhaps be 'hard cases', it is doubtful whether in many cases there will be any difference in consequence, if the correct approach to legal advice privilege is maintained.

The effect of the judgment in *Jet2.com* is that there will potentially be communications between legal advisers and the client, also sent or copied simultaneously to other individuals that, although part of the continuum of communication between lawyer and client, and despite having a relevant legal context, will not be privileged. In other words, the copying in of another individual or individuals into the email between lawyer and client may cause privilege to be lost. This reveals the controversial nature of imposing a dominant purpose requirement for legal advice privilege.

The Court of Appeal in *Jet2.com* also held that the question whether an attachment to an email is privileged is to be considered separately to the question whether the email itself is privileged.[102] That, too, is controversial.[103]

Litigation privilege 36.4

The leading modern statement of the scope of litigation privilege is contained in the speech of Lord Edmund-Davies in *Waugh v. British Railways Board*:

> *After considerable deliberation, I have finally come down in favour of the test propounded by Barwick C.J. in* Grant v. Downs*, 135 C.L.R. 674, in the following words, at p 677:*
>
> > *'Having considered the decisions, the writings and the various aspects of the public interest which claim attention, I have come to the conclusion that the court should*

102 ibid., paras. 104 to 108.

103 A similar issue arose in *The Financial Reporting Council v. Sports Direct International plc* [2020] 2 WLR 1256, in which the Court of Appeal rejected Sports Direct International's argument that legal advice privilege can be claimed in respect of a document that is not privileged in itself, because it is attached to an email sent by a client to a lawyer seeking advice or by a lawyer to a client giving advice.

© Law Business Research 2021

> *state the relevant principle as follows: a document which was produced or brought into existence either with the dominant purpose of its author, or of the person or authority under whose direction, whether particular or general, it was produced or brought into existence, of using it or its contents in order to obtain legal advice or to conduct or aid in the conduct of litigation, at the time of its production in reasonable prospect, should be privileged and excluded from inspection.'*
>
> *Dominant purpose, then, in my judgment, should now be declared by this House to be the touchstone.*[104]

Litigation privilege can therefore be described as the privilege of a client to withhold from disclosure:

- oral or written communications between the client or the lawyer (on the one hand) and third parties (on the other) or other documents created by or on behalf of the client or the lawyer;
- that come into existence once litigation is in contemplation or has commenced; and
- that come into existence for the dominant purpose of obtaining information or advice in connection with, or of conducting or aiding in the conduct of, such litigation.

36.4.1 Communications or other documents

Litigation privilege will apply to communications between the client or the lawyer and third parties for the relevant purpose. In the case of client–third party communications there is no requirement that the lawyer either requests the client to contact the third party[105] or that the communications are actually referred on to the lawyer.[106] In fact, no lawyer need have been engaged at the time of the communication.[107] In light of the narrow definition of 'client' in *Three Rivers No. 5*, as restrictively applied in subsequent decisions, many 'internal' communications within a corporation risk being characterised as communications between the client and 'third parties'. For example, where, as in *Three Rivers No. 5* itself, the corporation sets up a specific committee to deal with the relevant litigation, communications between a member of that committee and a non-committee employee of the corporation are likely to be characterised as communications between client and third party subject to

See Section 36.3.2.2

104 [1980] AC 521, 543, 544.

105 *Southwark and Vauxhall Water Company v. Quick* (1878) 3 QBD 315, 320 (*per* Brett LJ), 322 (*per* Cotton LJ).

106 ibid., at 320 (*per* Brett LJ), 323 (*per* Cotton LJ).

107 *Re Highgrade Traders Ltd* [1984] BCLC 151, 172 (*per* Oliver LJ); *Buttes Gas and Oil Co v. Hammer (No. 3)* [1981] QB 223, 243 (*per* Lord Denning MR).

© Law Business Research 2021

whether the employee is authorised to give instructions or receive advice on behalf of the corporation.

The privilege will also cover material, aside from communications, brought into existence in furtherance of the litigation purpose. The cases have traditionally spoken in terms of granting protection to the 'materials for the brief'.[108] A modern restatement of this principle is that, in an adversarial system 'each party should be free to prepare his case as fully as possible without the risk that his opponent will be able to recover the material generated by his preparations'.[109] As regards documents actually brought into existence by a client's lawyer, the better view is that these are in fact protected by legal advice privilege.[110] The 'materials for the brief' concept would apply to preparatory documents generated by the client that do not embody communications with third parties (such as a client's working notes or internal oral or documentary communications). Provided the document satisfies the other requirement of litigation privilege (as to which see below), it will also apply to a document generated for the purpose of being shown to a prospective adversary in circumstances where the document has not, or not yet, been shared with that adversary.[111]

See Section 36.3

Litigation commenced or in contemplation 36.4.2

In view of the underlying rationale of litigation privilege, the 'litigation' in question must be adversarial in nature.[112] Furthermore, the litigation must be 'reasonably in prospect'.[113] This matter was considered by the Court of Appeal in *USA v. Philip Morris Inc*.[114] In summary, it is not sufficient if there is simply a general apprehension of future litigation.[115] The requirement that litigation be 'reasonably in prospect' is not satisfied unless parties seeking to claim privilege can show that they were aware of circumstances that rendered litigation

See Section 36.2.3

108 *Southwark and Vauxhall Water Company v. Quick* (1878) 3 QBD 315, 320 (*per* Brett LJ); *Lyell v. Kennedy (No. 2)* (1883) 23 Ch D 387, 404 (*per* Cotton LJ).

109 *Three Rivers No. 6*, para. 52 (*per* Lord Rodger).

110 See also *Thanki*, paras. 2.56 to 2.60, 3.27.

111 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 102.

112 See *In re L (a Minor) (Police Investigation: Privilege)* [1997] AC 16 (HL) (litigation privilege was held to be inapplicable to the particular wardship proceedings in question, which were inquisitorial rather than adversarial in nature). The Upper Tribunal noted in *LM v. London Borough of Lewisham* [2009] UKUT 204 that *Re L* did not decide that there is never any litigation privilege in care proceedings but that their Lordships had confined themselves to cases where the filing of a report requires the leave of the court so that documents already filed in the proceedings may be disclosed to the expert or that the child may be examined.

113 *Hellenic Mutual War Risks Association (Bermuda) Ltd v. Harrison (The Sagheera)* [1997] 1 Lloyd's Rep 160, 166 (*per* Rix J); *USA v. Philip Morris Inc* [2004] EWCA Civ 330, CA, para. 68; *Three Rivers No. 6*, para. 83 (*per* Lord Carswell).

114 [2004] EWCA Civ 330.

115 ibid., para. 68.

© Law Business Research 2021

between themselves and a particular person or class of persons a real likelihood rather than a mere possibility; identifying potential causes of action and defendants to possible claims falls short of the necessary threshold.[116] By the same token, however, litigation need not be likely, in the sense of there being more than a 50 per cent chance of it occurring.[117]

The English courts apply a common-sense approach. Hence, litigation may be considered reasonably in prospect even if the cause of action has not yet arisen[118] or the party has not yet decided whether to take legal advice.[119] If litigation was reasonably in prospect when the communication or document was made, it does not matter if that litigation never commences.[120] Moreover, the litigation in which the privilege is later relied on need not concern the same subject matter or the same parties as the litigation in respect of which the privilege originally arose.[121]

The issue of when litigation may be said to be reasonably in contemplation was the subject of extensive consideration in *ENRC*. In that case, the defendant, ENRC, claimed litigation privilege in respect of documents created during the course of an investigation conducted by its lawyers that was initially prompted by a whistleblower report. The documents were created against the background of an anticipated criminal investigation by the SFO and during a period of engagement between the SFO and ENRC (which the SFO contended was part of a self-reporting process).

The judge at first instance, Andrews J, accepted that ENRC contemplated that it would be subject to a raid by the SFO, and that it reasonably contemplated a criminal *investigation* by the SFO, but found that this did not amount to anticipation of adversarial *litigation*.

Andrews J also rejected the submission that once ENRC contemplated a criminal investigation by the SFO, criminal prosecution was also in reasonable contemplation. In particular, she in effect drew a distinction between criminal and civil proceedings, finding that, for the purpose of a claim to litigation privilege where criminal proceedings are said to have been contemplated, the relevant party must have uncovered some evidence of wrongdoing before proceedings could be said to be in reasonable contemplation – otherwise there would be insufficient grounds for believing that a prosecution was likely.[122] She held that unless the relevant party had uncovered evidence of wrongdoing it could not consider the evidential test for the bringing of a criminal prosecution was likely

116 *Rawlinson & Hunter Trustees SA v. Akers* [2014] EWCA Civ 136, para. 24.

117 ibid., para. 65.

118 *Mayor and Corporation of Bristol v. Cox* (1884) 26 Ch D 678 (*per* Pearson J).

119 *Guinness Peat Properties v. Fitzroy Robinson Partnership* [1987] 1 WLR 1027, 1035, 1036 (*per* Slade LJ).

120 See *The Aegis Blaze* [1986] 1 Lloyd's Rep 203, 204 (*per* Parker LJ).

121 ibid., at 210.

122 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205 (Ch), para. 160.

© Law Business Research 2021

to be met.[123] The implication of that approach seemed to be that for a party to establish that litigation was a real likelihood, it was required to adduce evidence that was itself likely to betray the privilege being asserted and would tend to be self-incriminating (because it would need to identify matters discovered during the investigation leading it to believe that prosecution was likely and not merely possible). This approach (which had been the subject of much criticism following the first-instance decision in *ENRC*) was firmly rejected by the Court of Appeal, which found that the contemporaneous documents demonstrated that ENRC was aware of circumstances that rendered litigation between itself and the SFO a real likelihood rather than a mere possibility (so satisfying the test in *Philip Morris*), although uncertainty remained as to what the internal investigation would uncover. In particular, ENRC was in receipt of a whistleblower report making serious allegations of corruption and financial wrongdoing that it had appointed lawyers to investigate, and internal emails showed that senior figures within ENRC were anticipating an SFO raid and investigation. There had also been correspondence from the SFO where the subtext, so the Court found, was the possibility, if not the likelihood, of prosecution if the self-reporting did not result in a civil settlement. The Court indicated that, while not every manifestation of concern by the SFO is likely to be regarded as adversarial:

> *[W]hen the SFO specifically makes clear to the company the prospect of its criminal prosecution (over and above the general principles set out in the [Self-Reporting] Guidelines), and legal advisers are engaged to deal with that situation, as in the present case, there is a clear ground for contending that criminal prosecution is in reasonable contemplation.*[124]

Further, while it cannot be assumed that, once an SFO criminal investigation is reasonably in contemplation, so too is a criminal prosecution, on the facts of *ENRC* the evidence pointed clearly towards the contemplation by ENRC of a prosecution if the self-reporting process did not avert it. The Court of Appeal rejected the idea that because further investigations were required before a party could say with certainty that proceedings were likely that this would prevent proceedings from being in reasonable contemplation, and it rejected the judge's distinction between civil and criminal proceedings. Corporate parties who face the threat of SFO investigation and prosecution may take some comfort from the Court of Appeal's guidance: 'It would be wrong for it to be thought that, in a criminal context, a potential defendant is likely to be denied the benefit of litigation privilege when he asks his solicitor to investigate the circumstances of any alleged offence.'[125]

123 ibid., para. 151.

124 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 96.

125 ibid., para. 99.

© Law Business Research 2021

The Court of Appeal in *ENRC* also distanced itself from the decision of the Court of Appeal Criminal Division in *R (for and on behalf of the Health and Safety Executive) v Paul Jukes*.[126] In that case, the defendant had signed a statement shortly after a fatal industrial accident accepting that he was responsible for the company's health and safety. The Court in that case upheld the judge's decision that the statement was not covered by litigation privilege because criminal proceedings were not in contemplation and any privilege would anyway have attached to the company, which had not asserted it. The Court in *Jukes* had approved of Andrews J's distinction (at first instance in *ENRC*) between criminal and civil proceedings when considering whether proceedings were reasonably in contemplation. However, the Court of Appeal in *ENRC* held that *Jukes* was a decision on the facts and that the approval of Andrews J's approach was *obiter*. The effect of the decision of the Court of Appeal in *ENRC* is such that *Jukes* is likely to be marginalised and its apparent endorsement of Andrews J's approach to anticipation of litigation in a criminal context disregarded.

While the Court of Appeal's decision in *ENRC* has brought useful clarity as to the circumstances in which the first limb of the litigation privilege test may be satisfied, particularly in a corporate criminal context, there still remains some uncertainty as to exactly when regulatory proceedings may be regarded as sufficiently adversarial to meet the first limb. (The adversarial nature of the contemplated proceedings in *ENRC* was not in doubt, and the question of what type of regulatory action may engage litigation privilege was not directly addressed in *ENRC*). Some guidance can be found in *Tesco v. OFT*,[127] where the Competition Appeal Tribunal (CAT) was required to consider whether certain enforcement proceedings brought by the Office of Fair Trading (OFT) were 'litigation' for the purpose of claiming litigation privilege. The decision concerned the OFT's investigation into dairy retail price-sharing between various supermarkets and dairy processors. In September 2007, the OFT issued a statement of objections against a number of undertakings, including Tesco, alleging violation of the prohibition on anticompetitive agreements and practices. The OFT issued a supplemental statement of objections, in support of its case, in July 2009 and made its infringement decision in July 2011. On Tesco's appeal to the CAT, the OFT sought disclosure from Tesco of records of interviews with employees of other companies allegedly involved in Tesco's infringing conduct in the first half of 2011. Tesco resisted the application on the ground (among others) that the records were covered by litigation privilege.

The CAT refused the OFT's application for disclosure on the primary ground that such disclosure was not necessary, relevant and proportionate. However, it also considered the application of litigation privilege, finding that at the stage when Tesco contacted the potential witnesses the ongoing

126 [2018] Lloyd's Rep FC 157.

127 [2012] CAT 6.

© Law Business Research 2021

proceedings could properly be characterised as 'adversarial'. It was relevant that the statement, and supplementary statement, of objections had been issued and Tesco was contesting the allegations, that the OFT was determining Tesco's liability for a potential breach of the Competition Act and Tesco faced the possibility of a significant fine as a result, and that the proceedings were regarded as criminal for the purposes of Article 6 of the European Convention on Human Rights. The Chairman of the Tribunal also had regard[128] to the underlying rationale of fairness that underpins litigation privilege, finding that a fair procedure included the right of Tesco to present its case and to gather evidence, and that, as a corollary, litigation privilege applied to the relevant contacts with third-party witnesses.

The decision of the CAT confirmed that entitlement to claim litigation privilege in the context of regulatory enforcement proceedings will depend on the specific circumstances of the regulatory procedure and the stage it has reached. Passmore suggests that as a general rule one might have thought that a contested process in which the tribunal controlling the proceedings may make some sort of ruling that has mandatory consequences for a participant that are either penal (such as a prison sentence, a fine or other form of sanction such as a suspension from practice), or otherwise require the participant to do something he or she does not wish to do (such as pay damages, obey an injunction or give an undertaking not to do something), are ones in which the privilege should be available.[129] This must be right and is consistent with the decision of the Court of Appeal in *ENRC*: less significant than the precise stage an investigation by a regulator has reached is whether the client was aware of circumstances meaning that it reasonably contemplated adversarial proceedings ensuing.

Dominant purpose 36.4.3

The dominant purpose for the communication or the production of the relevant document must have been either to obtain information or advice in connection with the litigation or to conduct or assist in the conduct of it. However, in keeping both with the general language adopted by Lord Edmund-Davies in *Waugh's* case and the overriding rationale underlying litigation privilege, it must be understood as applying to documents and communications produced in many aspects of the litigation process.[130]

See Section 36.4

The test of 'dominance' is necessarily framed at a certain level of generality. Moreover, it is accepted that in applying it, the court will have to accept that 'human motivation is rarely linear'.[131] A dominant purpose has been described as the ruling, prevailing or most influential purpose – in other words, a purpose

128 ibid., para. 46.

129 *Passmore*, para. 3-156.

130 In support of this view, see *Passmore*, para. 3-134.

131 See to this effect *Esso Australia Resources Limited v. The Commissioner of Taxation* (1999) 201 CLR 49, para. 65 (*per* McHugh J), para. 93 (*per* Kirby J).

© Law Business Research 2021

that is of greater importance than any other.[132] As a consequence, a practical approach to ascertaining the pre-eminent purpose must necessarily be adopted. In particular, it is not necessary that it be the sole purpose. By the same token, however, it will not suffice if the relevant litigation purpose is merely a secondary, or co-equal, purpose.[133] The courts will examine 'purpose' from an objective standpoint,[134] looking at all the relevant evidence, including evidence of the relevant person's subjective purpose.[135] The relevant purpose is that of the 'instigator' of the document or communication in question.[136] There is sometimes scope for debate as to whether a number of related 'purposes' are properly to be regarded as one overall purpose or as distinct when applying the dominant purpose test. In *Bilta v. RBS*,[137] the various purposes of (1) providing information to Her Majesty's Revenue and Customs (HMRC) in accordance with RBS's duties as a taxpayer, (2) complying with RBS's Codes of Practice and (3) seeking to persuade HMRC to change its mind over a threatened tax assessment, were all held to be effectively subsumed within the dominant purpose of defeating the expected tax assessment. They were said to be part of the inseparable purpose of avoiding litigation if possible, such that the dominant purpose test was satisfied.[138] Similarly, in *ENRC*, there was an issue as to whether it was reasonable to regard ENRC's dominant purpose as being to investigate the facts to see what had happened and to deal with compliance and governance issues, or to defend the proceedings that were held to have been in reasonable contemplation at the time. The Court of Appeal held that:

> *[W]here there is a clear threat of a criminal investigation, even at one remove from the specific risks posed by the SFO should it start an investigation, the reason for the investigation of whistle-blower allegations must be brought into the zone where the dominant purpose may be to prevent or deal with litigation.*[139]

132 JD Heydon, *Cross on Evidence* (8th Australian ed., 2010), 891.

133 *Waugh v. British Railways Board* [1980] AC 521, 532 (*per* Lord Wilberforce); *Rawlinson & Hunter Trustees SA & Ors v. Akers & Anr* [2014] EWCA Civ 136; *Rawlinson & Hunter Trustees SA & Ors v. Director of the SFO* [2014] EWCA Civ 1129, para. 19.

134 *Price Waterhouse (a firm) v. BCCI Holdings (Luxembourg) SA* [1992] BCLC 583, 591 (*per* Millett J).

135 *Three Rivers No. 5*, para. 35.

136 *Victorygame Ltd v. Ahuja Investments Ltd* [2021] EWCA Civ 993, para. 48.

137 [2017] EWHC 3535 (Ch).

138 See also *Re Highgrade Traders* [1984] BCLC 151, 173 (*per* Oliver LJ). cf. *Financial Reporting Council Ltd v. Frasers Group Plc (formerly Sports Direct International Plc)* [2020] EWHC 2607 (Ch), in which Lord Justice Nugee held that reports produced by Deloitte concerning a proposed new accounting structure and its tax implications were not produced for the dominant purpose of litigation. See at paras. 30 to 39.

139 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 109.

© Law Business Research 2021

Further, the evidence showed that litigation was indeed the dominant purpose of the investigation. The Court's reasoning suggests that, where a party commences a factual investigation related to litigation that is reasonably in contemplation, a court will be inclined to accept that the contemplated litigation is the dominant purpose of that investigation rather than, for example, a purpose of simply establishing the material facts or dealing with compliance issues. It will be different, however, if the party in question is required by a specific policy to conduct an investigation, independent of any risk of litigation: in such a situation, the satisfaction of that policy requirement will be a distinct purpose that prevents the possible litigation from being the dominant purpose.[140]

The Court of Appeal in *ENRC* also considered an argument that the documents in question were not subject to litigation privilege because they were created in a period of co-operative dialogue between the SFO and ENRC and, so the SFO said, with the specific purpose of being shown to the SFO. The Court rejected this argument: the evidence did not support a finding that the documents were created with the specific purpose of being shown to the SFO, despite ENRC having stated to the SFO on a number of occasions that it intended to make 'full and frank disclosure' and to produce its investigation report.

The 'dominant purpose' issue was also considered by the Court of Appeal in *Rawlinson & Hunter Trustees SA v. Akers*.[141] In that case the claimants sought disclosure from the defendants, joint liquidators of certain companies in which the Tchenguiz family had an interest, of five reports prepared by Grant Thornton LLP that, the claimants said, had played a key role in the preparation of, and informed the content of, material placed before a judge in support of the application by the SFO for search warrants of the homes and business premises of Robert and Vincent Tchenguiz. The joint liquidators resisted disclosure on the ground of litigation privilege. Lord Justice Tomlinson explained that the identification of dominant purpose presented the biggest challenge, since 'plainly the first duty of the liquidators was to obtain information simply to establish what if any assets or liabilities existed and what if any steps were open to the liquidators to collect in the assets or to reduce or discharge the liabilities'.[142] The claim to privilege failed in circumstances where the evidence put forward by the joint liquidators in support of that claim failed to grapple with the need to establish which of dual or even multiple purposes was dominant. The dominant purpose must relate to the conduct of actual or contemplated litigation. This includes advice relating to avoidance of that litigation or its settlement once in train.[143]

The law on litigation privilege and dominant purpose seems to have taken a backwards step with the Court of Appeal's decision in *WH Holding v.*

140 *Waugh v. British Railways Board* [1980] AC 521.

141 [2014] EWCA Civ 136.

142 ibid., para. 15.

143 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, paras. 102, 118.

© Law Business Research 2021

E20.[144] The claimants, West Ham, had sued E20 over the number of seats in the London Olympic stadium that the football club was entitled to use. The decision concerned an application by West Ham for inspection of six emails over which E20 claimed privilege, passing between E20 board members, and between E20 board members and stakeholders. The emails were produced with the dominant purpose of discussing a commercial proposal for the settlement of the related dispute between E20 and West Ham in relation to rights arising under the concession agreement between the parties, which provided for West Ham to use the stadium for its home football matches. The Court of Appeal rejected E20's claim to privilege and held that litigation privilege does not extend to communications concerned with settlement that neither seek advice or information for the purposes of conducting litigation, nor reveal the nature of such advice or information. This is an undoubtedly narrower approach to assessing dominant purpose than was applied in *ENRC*, and adopts a much more restricted concept of the 'conduct' of litigation. The decision is also curious because it generates an inconsistency with the approach of without prejudice privilege. As the first instance judge noted, it gives rise to the anomalous position that a without prejudice offer made by one party to the other in litigation *would not be* before the court in a subsequent case, but any document recording the terms of the offer or its discussion, or the authorisation of the terms and putting of the offer, *would be* open to inspection. What is clear from this decision is that corporates will need to take great care when documenting internal settlement discussions or discussions to avoid litigation, if they wish to avert the risk of any subsequent application for disclosure, and where possible tie those discussions into legal advice so as to obtain the protection of legal advice privilege.

36.5 Common interest privilege

Common interest privilege (like joint interest privilege, which is not discussed here) can be said to be derivative insofar as it relies on establishing the existence of a primary ground of privilege (whether legal advice or litigation privilege) and then determining the circumstances in which multiple persons become entitled to assert it.

Common interest privilege arises in circumstances where party A voluntarily discloses a document that is privileged in its hands to party B, who has a common interest in the subject matter of the communication, or in the litigation in connection with which the document was produced.[145] Where this occurs, provided disclosure is given in recognition that the parties share

144 *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652.

145 See, generally, *Thanki*, paras. 6.18 to 6.24.

© Law Business Research 2021

a common interest,[146] the document will also be privileged in the hands of party B. Judicial formulation of this principle is found in the following terms:

> *[W]here a communication is produced by or at the instance of one party for the purposes of obtaining legal advice or to assist in the conduct of litigation, then a second party that has a common interest in the subject matter of the communication or the litigation can assert a right of privilege over that communication as against a third party.*[147]

The function of common interest privilege is not simply to prevent party A's privilege from being waived.[148] Where a common interest is made out, it enables party B actually to assert privilege as against a third party. Notwithstanding some terminological confusion, it seems that (unlike joint interest) common interest privilege, properly so-called, does not give party B the right to obtain disclosure of otherwise privileged documents from party A.[149] The rationale of common interest privilege can be explained as follows:

> *It is the communication in confidence to another interested party [in circumstances giving rise to a common interest] that requires the privilege to be available in respect of the document in his hands, whether or not he had the right to require that the document be disclosed to him.*[150]

In other words, common interest privilege is concerned with voluntarily shared privileged information. The aspect of voluntarism is important in understanding the limitations of common interest privilege.[151]

---

146 See *Newcrest Mining (WA) Ltd v. Commonwealth of Australia* (1993) 113 ALR 370, 372, Australian Federal Court.

147 *Winterthur Swiss Insurance Company and another v. AG (Manchester) Ltd (in liquidation) and others* [2006] EWHC 839 (Comm) (12 Apr. 2006), (*The TAG Group Litigation*) para. 78 (*per* Aikens J).

148 The fact that, independently of common interest, the disclosure of privileged material to third parties need not involve a broader loss of confidentiality or waiver of privilege is discussed in Section 36.8.

149 For support for this view, see *Thanki*, para. 6.21, as cited with approval (as it appeared in the previous edition of the book) by Newey J in *EMW Law LLP v. Halborg* [2017] EWHC 1014 (Ch), para. 50. cf. *Passmore*, para. 6-078. It is arguable that the point was misunderstood in *The TAG Group Litigation*, where it was held that 'common interest privilege' could operate as a 'sword' to obtain disclosure against party A as well as a 'shield' to deny disclosure to third parties. That case may be best understood as a case of joint interest privilege.

150 *Commercial Union Assurance Co plc v. Mander* [1996] 2 Lloyd's Rep 640, 645.

151 ibid., at 647, 648.

© Law Business Research 2021

It ought to follow that common interest privilege can be waived by the primary privilege holder.[152] This is the logical conclusion if common interest privilege involves the voluntary disclosure of information. It would be an undue fetter on the primary privilege holder to say that he or she cannot waive privilege without the consent of all those parties with whom he or she has chosen to share his or her advice. The position appears however to be a little more nuanced. In *Accident Exchange Ltd v. McLean*, Justice Andrew Smith considered that the *prima facie* position was, as with joint interest privilege and subject to any arrangement between the privilege holders, that one party sharing a document subject to common interest privilege should not be able to unilaterally deprive the others of the protection of privilege. The judge acknowledged that in cases of common interest privilege, the inference might more readily be drawn that the parties' arrangements were such that one privilege holder might waive privilege.[153] However, the judge found on the facts before him that the relevant contractual arrangements did not permit the party to waive privilege unilaterally.[154]

Furthermore, insofar as the proper focus of the doctrine is on the voluntary disclosure of privileged material by party A, it seems that the moment when a common interest must be established is when disclosure occurs.[155]

Although the doctrine is well established, its precise scope continues to be clarified. The doctrine of common (as distinct from joint) interest privilege was first recognised by the Court of Appeal in *Buttes Gas and Oil Co v. Hammer (No. 3)*.[156] A number of statements in that case indicated potential limitations to the doctrine, which, subsequent applications of it have clarified, do not in fact restrict its application.

---

152 See, for example, N Andrews, *English Civil Procedure* (2003), para. 27.63. cf. C Tapper, *Cross and Tapper on Evidence* (12th ed., 2010), 445, where it is stated, without citing any authority, that common interest privilege cannot be waived by one of the parties, without the authority of the other.

153 [2018] 4 WLR 26, para. 94.

154 ibid., para 95.

155 This point has not received detailed consideration. In The TAG Group Litigation, it seems Aikens J wrongly considered that the relevant time was when the privileged material was first created. However, insofar as he was considering the use of 'common interest' as a 'sword', it is arguable that his remarks should properly be understood as applying to cases of joint interest. Equally, in *Robert Hitchins Limited v. International Computers Limited* (10 Dec. 1996, CA), Peter Gibson LJ appeared to consider that a common interest could not be made out where such an interest did not exist at the time the material first came into being. However, it seems this did not affect the result in the case, which is probably best seen as a case of common interest privilege even though it was not decided on that basis. See *Thanki* at 6.20.

156 [1981] QB 223, CA. The Court of Appeal's decision was reversed on appeal. However, the House of Lords' ruling (see [1982] AC 888) left unaffected the issue of common interest privilege and the Court of Appeal's decision continues to be seen as the seminal authority for that doctrine.

© Law Business Research 2021

First, in *Buttes*, Lord Denning MR described common interest privilege as being 'a privilege in aid of anticipated litigation'.[157] While this confirms that one core application of the doctrine will be to circumstances in which a common interest arises out of parties' shared concerns regarding prospective litigation (discussed further below), it is now clear that the doctrine is not limited to this context. Hence in *Svenska Handelsbanken v. Sun Alliance and London Insurance plc*,[158] Justice Rix stated:

> *It seems to me that if legal advice obtained by one person is passed on to another person for the sake of informing that other person in confidence of legal advice which that person needs to know by reason of a sufficient common interest between them, then it would be contrary to the principle upon which all legal professional privilege is granted to say that the legal advice which was privileged in the hands of the first party should be lost when passed over in confidence to the second party, merely because it was not done in the context of pending or contemplated litigation.*

Support for the fact that common interest privilege can apply outside the context of anticipated litigation can also be found within Commonwealth authority.[159]

The second relevant aspect of *Buttes* concerns whether the parties to the common interest need to have retained the same lawyer (though not under a common retainer). Lord Justice Brightman expressed the doctrine (at page 267) in terms of the existence of 'a common interest and a common solicitor'. However, it does not appear that either of the other Lords Justice viewed the existence of a common lawyer as a requirement.[160] In some subsequent cases, deference has been paid to Brightman LJ's comments to the extent of suggesting that, while a common lawyer is not required, the commonality of interest requires that the parties could have used the same lawyer.[161] This has

157 Donaldson LJ (at pp. 251, 252) and Brightman LJ (at p. 267) each spoke of 'contemplated or pending litigation'.

158 [1995] 2 Lloyd's Rep 84 at p. 88.

159 See in particular *Unilateral Investments v. VNZ Acquisitions Ltd* [1993] 1 NZLR 468, 476, 478 (New Zealand High Court).

160 Donaldson LJ in fact pointed out (at pp. 251–52) that, in that particular case, the parties did not initially share a lawyer. Lord Denning also appears to have contemplated that the parties may have separate legal representation. This is implicit to his comments (at p. 243) that the parties may 'have consulted lawyers on the self-same points' and that each 'can collect information for the use of his or the other's legal adviser'.

161 See *Bank of Nova Scotia v. Hellenic Mutual War Risks Association (Bermuda) Ltd (Note)* [1992] 2 Lloyd's Rep 540, 542 (*per* Saville J); *USP Strategies plc v. London General Holdings Limited* [2004] EWHC 373 (Ch), para. 14, *The Times*, 30 April 2004 (*per* Mann J).

© Law Business Research 2021

also been put in terms of the retention of separate lawyers being a *prima facie* indication that the parties did not have the necessary common interest.[162]

However, even this limited expression of the need for a putative common lawyer has been criticised in the Australian authorities, in favour of a broader appraisal of common interest.[163] This also now appears to be the approach under English law.[164]

36.6 Without prejudice privilege

The 'without prejudice' rule applies to exclude all negotiations genuinely aimed at settlement from being given in evidence. As with legal professional privilege, no adverse inferences can be drawn against a party invoking the privilege.[165] The rule has two justifications:

- the public policy of encouraging parties to negotiate and settle their disputes out of court; and
- an implied agreement arising out of what is commonly said to be the consequences of offering or agreeing to negotiate without prejudice.[166]

The first justification is the prevailing justification and the second is now doubted and regarded as being at best of limited application.[167] In this context, 'settlement' means 'the avoidance of litigation'.[168] Therefore, the rule is not limited to negotiations aimed at resolving the legal issues between the parties but applies to any negotiations aimed at avoiding or reducing the scope of litigation, irrespective of whether they directly address or seek to resolve the relevant legal issues.

---

162 *Hellenic Mutual War Risks Association (Bermuda) Ltd v. Harrison* [1997] 1 Lloyd's Rep 160, 172 (*per* Rix J).

163 See *Bulk Materials (Coal Handling) Services Pty Ltd v. Coal and Allied Operations Pty Ltd* (1988) 13 NSWLR 689, 695 (*per* Giles J); *Network Ten Ltd v. Capital Television Holdings Ltd* (1995) 35 NSWLR 275, 282, Supreme Court of New South Wales (*per* Giles J).

164 In *Formica Ltd v. Export Credits Guarantee Department* [1995] 1 Lloyd's Rep 692, 699 Colman J framed the issue in the following terms: 'The protection by common interest privilege of documents in the hands of someone other than the client must pre-suppose that such third party has a relationship with the client and the transaction in question which, in relation to the advice or other communications, brings that third party within that ambit of confidence which would prevail between the legal adviser and his immediate client . . . the essential question in each case is whether the nature of their mutual interest in the context of their relationship is such that the party to whom the documents are passed receives them subject to a duty of confidence which the law will protect in the interests of justice'.

165 *Reed Executive plc v. Reed Business Information Ltd* [2004] 1 WLR 3026, para. 36.

166 See, for example, *Oceanbulk Shipping & Trading SA v. TMT Asia* [2011] 1 AC 662, paras. 24 and 27.

167 *Barnetson v. Framlington* [2007] 1 WLR 2443, para. 24.

168 *Forster v. Friedland* (CA, 10 Nov. 1992).

© Law Business Research 2021

The rule requires the existence of a dispute and an attempt to compromise it.[169] The crucial consideration is whether in the course of negotiations the parties contemplated or might reasonably have contemplated litigation if they could not agree.[170] The use of a 'without prejudice' heading on a letter is not decisive as to whether the privilege applies but does give rise to a rebuttable presumption that the document was intended to be a negotiating document.[171] If a letter is written in reply to a letter written without prejudice or is part of a continuing sequence of negotiations, it will be privileged and cannot be given in evidence without the consent of both parties.[172]

While there was previously some authority to suggest that the without prejudice rule only applied to prevent disclosure of 'admissions', it now appears to be settled that the rule is not limited in this way but that without prejudice discussions as a whole will be protected.[173]

The without prejudice rule is subject to a number of exceptions – it will not apply in the following circumstances:[174]

- *Unambiguous impropriety*: one party may be allowed to give evidence of what the other said or wrote in without prejudice discussions if the exclusion of the evidence would act as a cloak for perjury, blackmail or other 'unambiguous impropriety'.[175]
- *Proof, interpretation and rectification of an agreed settlement*: the rule will not operate to render inadmissible an actual compromise agreement. Without prejudice communications may also be admitted to determine whether a concluded compromise agreement was in fact reached, and what that agreement was.
- *Misrepresentation, fraud or undue influence*: evidence of without prejudice negotiations is admissible to show that an agreement apparently concluded between the parties during the negotiations should be set aside on the

169 *Bradford & Bingley plc v. Rashid* [2006] 1 WLR 2066, para. 81.

170 *Barnetson v. Framlingham Group* [2007] 1 WLR 2443 (CA).

171 *Thanki*, paras. 7.13, 7.14.

172 *Dixons Stores Group v. Thames Television* [1992] 1 All ER 349.

173 *Oceanbulk Shipping & Trading v. TMT Asia Limited* [2011] 1 AC 662, para. 27; *Somatra v. Sinclair Roche & Temperley* [2000] 1 WLR 2453, para. 22.

174 See *Thanki*, paras. 7.32 to 7.41; *Unilever plc v. The Procter & Gamble Co* [2000] 1 WLR 2436, 2444–45 (CA); *Oceanbulk Shipping & Trading v. TMT Asia Limited* [2011] 1 AC 662, paras. 30–33.

175 In *Motorola Solutions Inc v. Hytera Communications Cord Ltd* [2021] EWCA 11, the Court of Appeal emphasised that cases in which the unambiguous impropriety exception have been applied 'have been truly exceptional', and that a 'good arguable case' or a 'plausible evidential basis' for asserting that the exception applies will not be sufficient. The Court held at para. 64: 'the test remains one of unambiguous impropriety. Nothing less will do. That is a test which, deliberately, is difficult to satisfy. . . . In view of the necessary limits to the conclusions which a court can reach at an interim stage, the existence of a credible dispute about what was said (or what was meant by what was said) may mean that a court cannot be satisfied that there has been an unambiguous impropriety and therefore does not admit the evidence'.

© Law Business Research 2021

ground of misrepresentation, fraud or undue influence. It has been held recently that such evidence may also be admitted to *rebut* allegations of misrepresentation and fraud and thereby uphold the parties' agreement.[176]

- *Estoppel*: where an estoppel founded on a statement made in without prejudice negotiations is alleged, the relevant without prejudice material will be admissible to determine the existence of the estoppel.
- *Reasonableness of mitigating steps*: where there is an issue as to whether a party has acted reasonably to mitigate loss in the conduct and conclusion of negotiations for a settlement the without prejudice material may be examined for that purpose.
- *Delay*: evidence of negotiations may be given to explain delay or apparent acquiescence.

Since the without prejudice privilege belongs to both parties, it cannot be waived without both parties' consent, at least in the context of civil litigation.[177] This is because it is categorised as a joint privilege.[178] However, there is now some limited authority for the proposition that a party to negotiations with a regulatory authority may unilaterally waive without prejudice privilege in respect of communications with that authority if it subsequently puts the basis of the regulator's decision in issue in civil proceedings.

The law took an unusual and unexpected turn in this direction with the decision of Justice Birss in *Property Alliance Group Ltd v. Royal Bank of Scotland plc*.[179] The case concerned alleged LIBOR fixing by RBS employees. The claimant, PAG, had purchased interest rate swaps from Royal Bank of Scotland (RBS) in 2004–2008 that had been referenced to GBP LIBOR. PAG claimed that it had entered into the swaps in reliance on certain misrepresentations to the effect that RBS was not rigging LIBOR (PAG also relied on alleged implied terms to that effect). In support of its plea that the representations were false, PAG referred to the contents of the final notice issued by the Financial Services Authority (FSA), the predecessor body to the FCA, against RBS, which had found that RBS had manipulated Swiss Franc LIBOR and Japanese Yen LIBOR, but otherwise made no findings in relation to other currency denominations. The FSA final notice had been issued following a settlement reached between RBS and the FSA.

In its defence, RBS admitted that it had manipulated Swiss Franc LIBOR and Japanese Yen LIBOR but denied any wrongdoing in relation to GBP LIBOR. In support of that denial, RBS pleaded: 'For the avoidance of doubt,

176 *Berkeley Square Holdings v. Lancer Property Asset Management Ltd* [2021] EWCA Civ 551.

177 *Walker v. Wilsher* (1889) 23 QBD 335, at 337; *Reed Executive plc v. Reed Business Information Ltd* [2004] 1 WLR 3026, para. 19.

178 D Vaver, 'Without Prejudice Communications – their admissibility and effect' (1974) 9 *UBC Law Review* 85, at p. 105; Heydon, *Cross on Evidence* (10th edn) [25350].

179 *Property Alliance Group Ltd v. Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch).

© Law Business Research 2021

there have been no regulatory findings of misconduct on the part of RBS in connection with GBP LIBOR.'

PAG sought disclosure of a wide range of documents over which RBS claimed both without prejudice privilege and also legal professional privilege.[180] RBS claimed that communications passing between it and the FSA between December 2012 and January 2013 were subject to without prejudice privilege on the grounds that they recorded negotiations with a view to the settlement announced in February 2013. The FCA wrote a letter in support of RBS's claim to without prejudice privilege on the grounds of public interest.

The judge rejected RBS's right to withhold disclosure of these documents. He held that by pleading in its defence that the regulators had not found any misconduct relating to GBP LIBOR, RBS 'had itself put in issue the basis on which the regulatory findings were made',[181] and as a result RBS had to give disclosure of the communications.[182] The judge's reasoning, while difficult to discern, appears to have been that communications on which the settlement was based might have been incomplete, mistaken or misleading.[183] As he explained:

> *If the communications on which the Final Notice was based were false, then to allow RBS to rely on what is absent from the Final Notice but at the same time to withhold inspection of those communications would compound the falsehood. That will not do.*[184]

PAG argued that the sort of regulatory context in which the communications between RBS and the FSA took place was not within the without prejudice rule.[185] Birss J rejected the submission that the without prejudice rule was inapplicable, finding that 'the public policy on which the without prejudice rule is based is capable of applying in order to promote the settlement of FCA investigations',[186] but suggested that there is a particular kind of privilege covering settlement negotiations between firms and the FCA (and presumably therefore other regulators) that is 'analogous with' but 'not identical to' without prejudice privilege.[187] Unlike the normal without prejudice rule (where the consent of both parties is required for any waiver of the privilege), this

180 RBS relied on the doctrine of limited waiver. The part of the decision dealing with limited waiver is uncontroversial and consistent with previous authority (see Section 36.8.1).

181 *Property Alliance Group Ltd v. Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch), para. 94.

182 For the same reason – namely that RBS had 'put in issue' the basis on which regulatory findings were made – Birss J held that RBS was not entitled to withhold from inspection the six privileged documents that it had shared with regulators (see para. 114). This aspect of the decision is discussed below at Section 36.8, but must be wrong.

183 *Property Alliance Group Ltd v. Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch), para. 92.

184 ibid., para. 96.

185 ibid., para. 59.

186 ibid., para. 87.

187 ibid., para. 99.

© Law Business Research 2021

'analogous' type of without prejudice rule could, according to Birss J, be waived unilaterally by RBS putting the basis on which a final notice was decided in issue in civil proceedings, without the consent of the FCA. This decision is difficult to understand, in particular why the judge decided he needed to fashion a new type of privilege and why this new type of without prejudice privilege is apparently capable of being waived unilaterally.

In the event, RBS applied to amend its defence so as to remove the paragraph that Birss J had held put in issue the basis of the FSA's findings. Birss J held that by doing so RBS could prevent the waiver that had been identified in his earlier judgment from taking place.[188] He held that it was open to a party to decide not to rely on privileged material and therefore amend the relevant pleading, in which case, if the amended pleading was permitted, no waiver would have taken place merely by virtue of having been pleaded previously. Any substantive need for RBS to appeal on the waiver aspect of the first decision of Birss J, therefore, fell away (and RBS's appeal in relation to other aspects of the decision was in any event settled). The law has accordingly been left in a state of some uncertainty on this topic.

36.7 Exceptions to privilege

36.7.1 The crime-fraud exception

See Section 36.7.2

Aside from certain very limited statutory exceptions where privilege may exceptionally be overridden, the principal situation[189] where communications may not be protected by privilege is the crime-fraud exception. In broad terms, this exception provides that there is no privilege in documents or communications that are themselves part of a crime or a fraud, or that seek or give legal advice about how to facilitate the commission of a crime or a fraud. This exception applies to both legal advice privilege and litigation privilege.[190]

188 [2015] EWHC 3272 (Ch), para. 69.

189 The Court of Appeal held in the case of *R v. Brown (Edward)* [2016] 1 WLR 1141 that in addition to the fraud/iniquity exception, the normally absolute rule of privilege is capable of further qualification at common law. The Court of Appeal held that it was appropriate, in what was likely to be an extremely narrow band of cases and by way of an additional common law qualification or exception to the inviolable nature of legal professional privilege, to impose a requirement that particular individuals could be present at client–lawyer discussions if there was a real possibility that the discussions were to be misused for a purpose and in a way involving impropriety amounting to an abuse of the privilege that justified interference. In this case, it was appropriate for two nurses to be present with and handcuffed to the appellant, who was in detention in a high security psychiatric hospital, when he consulted with his lawyers because there was reason to think he would otherwise take that opportunity to harm himself or others.

190 *Dubai Aluminium Co Ltd v. Al Alawi* [1999] 1 WLR 1964; *Dubai Bank v. Galadari (No. 6), The Times* (22 Apr. 1991); *Kuwait Airways Corporation v. Iraqi Airways Company* [2005] 1 WLR 2734.

© Law Business Research 2021

It is important to bear in mind the truly exceptional nature of the crime-fraud exception. A court will not lightly deprive a party of the fundamental protection of legal professional privilege,[191] particularly where the privilege is challenged on an interlocutory application.[192] The reason for such caution is plain: once the court determines that the veil of privilege is to be lifted, and that the privileged documents are to be disclosed, there is no return. The holder's right to privilege will have been irretrievably destroyed.

The solicitor need not be involved in the crime or fraud for the exception to apply: the solicitor may be wholly innocent.[193]

Notwithstanding its exceptional nature, it may be that regulators or prosecutors in certain circumstances will wish to challenge a party's claim to privilege on the basis of this exception. To successfully challenge that claim the regulator or prosecutor will need to establish that:

- there was a specific dishonest criminal (i.e., fraudulent) purpose; and
- the privileged material was produced in furtherance of or in preparation for that purpose.[194]

As to the evidential burden on the party invoking the exception, there must be some *prima facie* evidence of the crime or fraud; a mere allegation or charge of crime or fraud is not sufficient.[195] In a case where the crime or fraud relied on is one of the issues in the action, the applicable standard may be the 'very strong *prima facie* case', whereas in a case where the issue of fraud is freestanding, it may be sufficient to establish a 'strong *prima facie* case'.[196] But ultimately each case must be decided on its own facts.[197]

---

191 *R v. Cox and Railton* (1884) 14 QBD 153, 176.

192 *Derby & Co Ltd v. Weldon (No. 7)* [1990] 1 WLR 1156, 1173.

193 *Banque Keyser Ullman SA v. Skandia (UK) Insurance Co. Ltd* [1986] 1 Lloyd's Rep 336, 337.

194 *Butler v. Board of Trade* [1971] 1 Ch 680, 689C (*per* Goff J): 'What has to be shown prima facie is not merely that there is a *bona fide* and reasonably tenable charge of crime or fraud but a prima facie case that the communications in question were made in preparation for or in furtherance or as part of it.'

195 *O'Rourke v. Darbishire* [1920] AC 581, 604, 614; *Derby & Co v. Weldon* (No. 7) [1990] 1 WLR 1156, 1166.

196 *Kuwait Airways Corporation v. Iraqi Airways Corp* (No. 6) [2005] 1 WLR 2734, para. 42 (*per* Longmore LJ).

197 *Derby & Co Ltd v. Weldon* (No. 7) [1990] 1 WLR 1156, 1173. In the recent case of *Addlesee v Dentons Europe LLP* [2020] EWHC 238 (Ch), Master Clark held that the 'strong *prima facie* case' standard, rather than the 'very strong' standard, should apply, even though the alleged fraud was in issue in the action. The Master held at paras. 45 to 48 that (1) the distinction between a 'strong' and 'very strong' *prima facie* case is 'not readily discernible' in practice; (2) on the facts of *Kuwait Airways*, where the 'very strong' test was adopted by Longmore LJ, that higher test was satisfied (para. 39) so Longmore LJ's statement at para. 42 that 'I would myself use the words "very strong"' was strictly *obiter*; (3) in *Dubai Aluminium Co Ltd v. Al-Alawi* [1999] 1 WLR 1964, a case approved in *Kuwait Airways*, the 'strong *prima facie* case' standard was applied; and (4) 'most importantly', *Kuwait Airways* was not inconsistent

© Law Business Research 2021

There is some debate as to the proper scope of the exception. In the authors' view, being an exceptional principle, the crime-fraud exception ought to apply only in circumstances where the conduct in question amounts to a crime or a fraud (i.e., involving an element of dishonesty).[198] There is, however, some suggestion in some texts and cases that the scope of the exception has been broadened to cases arguably not involving crime or fraud (which has also led to the exception often being termed the 'iniquity exception').

The widening of the exception to encompass conduct falling short of dishonesty is said to emanate from the Court of Appeal's decision in *Barclays Bank v. Eustice*.[199] However, it is doubtful that *Eustice* should be taken as authority for extending the scope of the crime-fraud extension. Though using the language of 'iniquity', in the context of civil proceedings, the Court of Appeal nonetheless was clear that the impugned conduct was a type of fraud (in this case, on the creditors), within the meaning of section 423 of the Insolvency Act 1986. Equally, in *JSC BTA Bank v. Ablyazov*, Justice Popplewell characterised Mr Ablyazov's conduct in terms of concealment and deceit, namely as dishonest and fraudulent.[200] Potentially more contentious is *Barrowfen Properties v Patel*, where Tom Leech QC, sitting as a judge of the Chancery Division, held that the iniquity exception is engaged where allegations of breaches of fiduciary duty 'involve fraud, dishonesty, bad faith or sharp practice or where the director consciously or deliberately prefers his or her own interests over the interests of the company and does so "under a cloak of secrecy"'.[201] On the facts of that

---

with the analysis in *Derby v. Weldon* that each case must be judged on its own facts. In the particular circumstances of *Addlesee*, including that the material before the Master was 'substantially identical to that which will be before the trial judge' and that the defendant (not itself a party accused of fraud, but the former solicitor of those parties) did not deny the fraud but simply did not admit it, the Master held that the 'strong *prima facie* case' standard was to be applied. (In any event, the Master's conclusion on the facts of that case was that the claimants had shown not only a 'strong *prima facie* case' of fraud, but a 'very strong and compelling case': para. 144).

198 *Crescent Farm (Sidcup) Sports Ltd v. Sterling Offices Ltd* [1972] Ch 553, 565 (*per* Lord Goff); *Gamlen Chemical Co (UK) Limited v. Rochem Ltd* (No. 2) 7 December 1979 (CA).

199 [1995] 1 WLR 1238. See, for example, *Accident Exchange Ltd v. McLean* [2018] 4 WLR 26, where the judge cited *Eustice* for the proposition that the iniquity exception 'applies not only in cases of fraud, but more generally where wrongdoing or iniquity is sufficient to set aside legal professional privilege'.

200 [2014] EWHC 2788 (Comm), para. 98: 'The evidence establishes at least a very strong *prima facie* case that from the moment Mr Ablyazov engaged Clyde & Co he was bent on a strategy of concealment and deceit in relation to his assets which would involve perjury, forgery and contempt as and when such was required for that purpose.' In *Akhmedova v. Akjmedov* [2020] 4 WLR 15, Gwynneth Knowles J noted at para. 26 that the question of what sort of wrongdoing engages the crime-fraud exception is 'somewhat vexed', but that, in the circumstances of that case, it was sufficient to observe that the exception will be engaged by the devising of a scheme to dissipate assets so as to frustrate enforcement of an anticipated judgment.

201 [2020] EWHC 2536 (Ch), para. 35.

© Law Business Research 2021

case, the alleged conduct was held to amount, 'without question', to 'fraud (in the wide sense), dishonesty or bad faith'.[202] But more broadly, if the formulation adopted in *Barrowfen Properties* is correct (which might be questioned), it may open the way for the crime-fraud exception to be invoked in other cases, where a director has acted in breach of duty, has prioritised his or her own interests over those of the company, and has acted without the knowledge of others ('under a cloak of secrecy'), but where those actions were not necessarily fraudulent or dishonest.[203]

Even if, contrary to the above, *Eustice* is understood as having extended the crime-fraud exception to conduct falling short of dishonesty, the basis for such extension is dubious, being based on an authority – *Ventouris v. Mountain*[204] – that was not about the crime-fraud exception at all. Indeed in *McE v. Prison Service of Northern Ireland*,[205] Lord Neuberger left open the question as to whether *Eustice* had been correctly decided.

The Court of Appeal was invited to consider this issue in *Curless v. Shell* but declined to offer any view, finding that it is 'an important argument, which will no doubt have to be decided one day; but not in this case'.[206]

A further issue can arise where the alleged dishonest purpose is that of a third party, rather than the privilege holder. The decision of the House of Lords in *R v. Central Criminal Court, ex p Francis & Francis*,[207] followed in *BBGP Managing General Partner Limited v. Babcock and Brown*,[208] suggests that it may be sufficient if a criminal or dishonest purpose of a third party can be established to the requisite evidential standard. It has also been held, in reliance on *Francis & Francis*, that an innocent client or privilege holder can only lose the protection of privilege because of the iniquity of a third party if there is a relationship or 'nexus' between the third party and the privilege holder that is used by the third party to advance the wrongdoing such that the privilege holder can be described as the wrongdoer's 'tool'.[209]

However, a situation that remains untested is where the privilege holder is a company, and dishonest or criminal conduct is alleged against that company,

202 ibid., para. 55.

203 On the other side of the coin, the Court of Appeal in the recent case of *Victorygame Ltd v. Ahuja Investments Ltd* [2021] EWCA Civ 993 appears to have assumed that the crime-fraud exception applied only where there had been behaviour 'of a criminal nature', or, perhaps, 'closely akin to it': paras. 57, 58. See further, for recent examples of approaches taken by the High Court to the crime-fraud exception: *Hotel Portfolio II UK Ltd v. SMA Investment Holdings Ltd* [2019] EWHC 1754 (Comm) at paras. 32 to 33 and *Various Claimants v. News Group Newspapers Limited* [2021] EWHC 680 (Ch) at para. 4.

204 [1991] 1 WLR 607.

205 [2009] 1 AC 908, para. 109.

206 *Curless v. Shell Limited* [2019] EWCA Civ 1710, para. 60.

207 [1989] 1 AC 346.

208 [2011] Ch 296.

209 *Accident Exchange Ltd v. McLean* [2018] 4 WLR 26, paras. 33 to 38 and 48 to 49.

© Law Business Research 2021

but a dishonest or criminal purpose can only be established to the requisite evidential standard against certain individuals. It is suggested that the requirements for establishing the crime-fraud exception are likely to present some difficulty for regulators and prosecutors in such a situation, where it is unlikely that the company – which stands accused of dishonesty or criminal conduct – can be regarded as an innocent 'tool'. In particular, it does not follow that because the criminal or fraudulent purposes of one or more individuals can be established, the necessary fraudulent purpose of the corporate is established. Whether it can be, will depend on complex issues of attribution and the doctrine of identification in the criminal context.

A case of particular interest in the regulatory context is *CITIC Pacific Ltd v. Secretary for Justice and anor*,[210] in which the Hong Kong Court of Appeal considered the application of the crime-fraud exception in the context of alleged fraud and breach of listing rules by a company (CITIC) listed on the Hong Kong Stock Exchange. Hong Kong's Securities and Futures Commission (SFC) had commenced investigating why CITIC had delayed a profit warning in October 2008, during the financial crisis. As part of its investigation into alleged 'defalcation, fraud, misfeasance and other misconduct' on the part of CITIC's management, the SFC sought various documents, including privileged documents, which CITIC subsequently provided to it. The police commenced criminal investigations and CITIC learned that the SFC had passed the privileged documents to the United States Department of Justice (DOJ) for use in the criminal proceedings. CITIC issued an application for an order that the privileged documents be returned on the basis that privilege had been waived for the limited purpose only of the SFC investigation. The application was resisted by the DOJ, *inter alia*, on the basis that the documents were created by certain of the persons responsible for the management of CITIC for the purposes of the fraud, such that the crime-fraud exception applied.

The Court of Appeal (reversing the decision of Justice Wright) found that the crime-fraud exception had not been made out since there needed to be evidence of a fraudulent purpose behind the seeking and obtaining of the advice by the relevant directors of CITIC, which had not been established, for there to be the necessary causal relationship between the advice received and the fraudulent conduct.

The decision in *CITIC* is instructive in demonstrating a cautious approach by an appellate court to the encroachment of legal professional privilege where the crime-fraud exception is invoked by a prosecuting authority in the context of, and (presumably) in aid of, anticipated criminal proceedings.

210 [2012] 2 HKLRD 701.

© Law Business Research 2021

Statutory and other exceptions 36.7.2

Previously, the courts did not require a great deal of persuasion that Parliament had intended to override legal professional privilege.[211] That is no longer the case.[212] For example, statutory powers requiring the production of documents would generally be deemed to exclude the right to demand documents subject to legal professional privilege. Any exception to this rule would have to be explicitly supported by primary legislation.[213] Explicit support would require clear language or necessary implication. A necessary implication in this area is not an exercise in interpretation; it is a matter of express language and logic.[214] A necessary implication arises only where the legislative provision would be rendered inoperative or its object largely frustrated in its practical application if the privilege were to prevail.[215] Any curtailment of privilege could only be to the extent reasonably necessary to meet the ends that justify the curtailment.[216]

For a time there appeared to be a further exception[217] to legal professional privilege where a professional was under investigation by their regulator seeking production of documents over which the professional's client could claim privilege, or the professional wished to produce the documents to show the regulator that he or she had behaved properly (i.e., 'underlying client-privileged documents' rather than documents over which the professional could claim his or her own privilege).[218] There were *dicta* in a number of cases suggesting that those documents could be disclosed to the regulator without the client's consent, though the regulator would not be permitted to use them against the underlying client and was required to take steps to protect the underlying client's confidential privileged material. The justification for the

---

211 See, for example, *R v. Inland Revenue Commissioners, ex p Lorimer* [2000] STC 751.

212 Although *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, HL is regarded as the landmark ruling in this area, *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532, paras. 5, 31, HL is of equal significance. These cases applied the more general principle that a statute is generally not intended to override fundamental rights: *R v. Secretary of State for the Home Department, ex p Simms* [2000] 2 AC 115, 131, HL; *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, paras. 96 to 97, HL (*per* Lord Carswell).

213 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 8; *General Mediterranean Holdings SA v. Patel* [2000] 1 WLR 272; *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532; *Bowman v. Fels* [2005] 1 WLR 3083, paras. 70 to 91, CA. See also *Baker v. Campbell* (1983) 153 CLR 52.

214 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 45 (*per* Lord Hobhouse).

215 *Daniels Corporation International Pty Ltd v. Australian Competition and Consumer Commission* (2002) 213 CLR 543, para. 43 (*per* McHugh J).

216 *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532, paras. 5 (*per* Lord Bingham) and 31 (*per* Lord Cooke).

217 Though it had been argued that it was not truly an 'exception' because the client's privilege in the relevant material was not infringed.

218 See *Thanki*, paras. 4.91 to 4.96.

© Law Business Research 2021

rule was said to be either that there was no infringement of the underlying client's privilege where the documents were not to be used against him or her, or that, if there was an infringement, it was of a technical nature that may be authorised without satisfaction of the usual 'clear language or necessary implication' test.[219] This issue was considered by the Court of Appeal in *The Financial Reporting Council Limited v. Sports Direct International Plc*.[220] The Financial Reporting Council (FRC), which, among other things, is the regulator for statutory auditors in the United Kingdom, had used its statutory powers to seek the production of certain documents from Sports Direct for the purpose of its investigation into its statutory auditor. Sports Direct withheld the documents on grounds of legal professional privilege and the FRC challenged this, relying on the principle that it, as regulator, was entitled to obtain those documents from Sports Direct, even if they were documents over which Sports Direct had a valid claim to privilege, as long as it did not use those documents against Sports Direct. At first instance, the judge, while acknowledging that the issue was 'difficult', agreed with the FRC and ordered that the documents be produced.[221] He summarised the principle as follows:

> *[T]he production of documents to a regulator by a regulated person solely for the purposes of a confidential investigation by the regulator into the conduct of the regulated person is not an infringement of any legal professional privilege of clients of a regulated person in respect of those documents. That being so, in my judgment the same must be true of the production of documents to the regulator by a client.*[222]

The Court of Appeal reversed this decision, finding that there is no such principle.[223] The task of the court is to apply the test laid down by the House of Lords and Privy Council (respectively) in *Morgan Grenfell*[224] and *B v. Auckland*,[225] by looking at the relevant legislation that is the source of the statutory power to obtain documents to see whether Parliament must have intended to override the privilege.

One of the most significant statutory exceptions in the regulatory context is covert surveillance under the Regulation of Investigatory Powers Act 2000.[226] However, if covert surveillance is likely to result in the acquisition of knowl-

219 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 32 (*per* Lord Hoffmann).

220 [2020] 2 WLR 1256.

221 [2019] 2 All ER 974, paras. 57 to 92.

222 ibid., para. 84.

223 [2020] 2 WLR 1256, para. 24.

224 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563.

225 *B v. Auckland District Law Society* [2003] 2 AC 736.

226 See *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908. Other limited statutory exceptions are set out in *Thanki*, para. 4.90.

© Law Business Research 2021

edge of matters subject to legal professional privilege, the appropriate authorisations or approval cannot be made unless there are exceptional and compelling circumstances. Unless that risk can be entirely removed, steps must be taken to ensure that any such information will not be used for the purpose of further investigations or during the course of any subsequent criminal trials.[227]

It has also previously been suggested that there is an exception to legal advice privilege in that it does not extend to a communication containing information that the client instructs the solicitor to repeat. The Court of Appeal has now confirmed that there is no such exception.[228]

Loss of privilege and waiver 36.8

Although privilege, once established, will endure indefinitely, it may be lost, principally in two ways. First, the party entitled to assert privilege may waive the right. This can occur expressly, for example, by choosing to place privileged material before the court. For this purpose, the partial disclosure of a privileged document will usually involve a waiver of privilege in respect of the whole document.[229] Waiver will also occur by necessary implication in certain proceedings (implied waiver). For example, where a client sues a lawyer, the client will be taken impliedly to waive privilege in respect of those documents arising under the retainer subject to dispute.[230]

The second principal circumstance in which privilege will be lost is where there is a loss of confidentiality. As discussed in Section 36.2.1, the confidentiality of the communication or document is a condition precedent to its being privileged. However, the significance of this requirement should not be misunderstood. It is well established that a privileged document does not lose its quality of confidence simply because it is disclosed to persons other than the client and the lawyer. Plainly, if a document has been made available to the general public, all confidence (and with it privilege) will have been lost.[231] Where a document is read or referred to in a public court hearing, the question whether confidentiality in the document itself (as opposed to information within the document) is lost is a matter of degree.[232] Where privileged material

227 *R v. Turner (Elliott Vincent)* [2013] EWCA Crim 643.

228 *Raiffeisen Bank International v. Asia Coal Energy Ventures Ltd* [2020] 1 WLR 2298.

229 *Great Atlantic Insurance Co. v. Home Insurance Co.* [1981] 1 WLR 529.

230 See *Paragon Finance v. Freshfields* [1999] 1 WLR 1183. An implied waiver may, however, be limited: see *Eurasian Natural Resources Corporation v. Dechert* [2016] EWCA Civ 375.

231 See (in the general context of an action for breach of confidence) *Attorney-General v. Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109, 177, where Sir John Donaldson MR said: 'As a general proposition, that which has no character of confidentiality because it has already been communicated to the world, i.e., made generally available to the relevant public, cannot thereafter be subjected to a right of confidentiality: *O. Mustad & Son v. Dosen* (Note) [1964] 1 WLR 109. However, this will not necessarily be the case if the information has previously only been disclosed to a limited part of that public.'

232 *SL Claimants v. Tesco Plc* [2019] EWHC 3315 (Ch), para. 42.

© Law Business Research 2021

is disclosed to a limited number of third parties in circumstances expressly or impliedly preserving the overall confidentiality as against the rest of the world, privilege will be maintained. This point is well illustrated by an example cited with approval by the English courts:

> *If A shows a privileged document to his six best friends, he will not be able to assert privilege if one of the friends sues him because the document is not confidential as between him and the friend. But the fact six other people have seen it does not prevent him claiming privilege as against the rest of the world.*[233]

It has therefore been accepted that where a client disseminates a record of privileged material, either within its own corporation or to third parties, confidentiality will not necessarily be lost.[234] It is a separate question whether the party to whom the documents are disclosed acquires a right to assert privilege by virtue of a common interest.

See Section 36.5

As noted above in Section 36.6, in *Property Alliance Group Ltd v. Royal Bank of Scotland plc*,[235] it was suggested that privilege can be lost by a party putting something in issue. This aspect of the decision must be wrong: legal professional privilege is absolute unless waived or overridden by statute. There is no balancing act to be carried out with some competing public interest. It may be that the reference to putting something in issue was a confusion with the doctrine of collateral waiver. However, collateral waiver, discussed below, requires some form of 'deployment' of the privileged material, not simply that a relevant matter is put in issue.

See Section 36.8.2

In *Raiffeisen Bank International v. Asia Coal Ventures*,[236] the Court of Appeal confirmed that a statement by a solicitor to a third party as to the instructions he or she has from a client does not automatically and without more give rise to a loss of confidentiality in the documents that contain or evidence those instructions. However, privilege will be waived if the client puts in issue the content of those instructions. Again, it is suggested that this must be understood as meaning that privilege will be waived if the client relies on the content of the instructions in a way that gives rise to a waiver in accordance with established principles concerning implied and collateral waiver, as discussed below.

36.8.1 Limited waiver

Limited waiver is achieved where a party discloses a privileged document, or communicates privileged information, to a limited number of third parties in

233 *USP Strategies v. London General Holdings* [2004] EWHC (Ch) 373, para. 19 (*per* Mann J); *Gotha City v. Sotheby's* [1998] 1 WLR 114, CA, para. 119 (*per* Staughton LJ).

234 *Gotha City v. Sotheby's* [1998] 1 WLR 114, CA; *USP Strategies v. London General Holdings* [2004] EWHC (Ch) 373.

235 [2015] EWHC 1557 (Ch).

236 [2020] 1 WLR 2298.

© Law Business Research 2021

circumstances expressly or impliedly preserving the overall confidentiality of the document or information as against the rest of the world. It is well established that in such circumstances the disclosing party does not lose privilege in the document.[237]

Limited waiver may frequently arise in a regulatory context. In *B v. Auckland District Law Society*,[238] in the course of investigating a complaint against a law firm, certain privileged documents had been handed over to counsel appointed by The Law Society. The letter handing over the documents stated that the documents were made available to counsel for the limited purposes of the investigation and 'on the express basis that in doing so privilege is not waived'. The Law Society sought to use the documents in subsequent disciplinary proceedings brought against the law firm, on the basis that the privilege had been 'let out of the bag'. The Privy Council rejected this submission. Lord Millett held:

> *It does not follow that privilege is waived generally because a privileged document has been disclosed for a limited purpose only. . . . The question is not whether privilege has been waived, but whether it has been lost. It would be unfortunate if it were. It must often be in the interests of the administration of justice that a partial or limited waiver of privilege should be made by a party who would not contemplate anything which might cause privilege to be lost, and it would be most undesirable if the law could not accommodate it.*[239]

There was further development of the limited waiver doctrine in *Berezovsky v. Hine*.[240] Mr Berezovsky's lawyers had sent privileged draft witness statements in relation to Mr Berezovsky's action against Mr Abramovich to solicitors acting for his friend, Mr Patarkatsishvili, in an asylum application as it was thought they might be useful. Mr Patarkatsishvili died and his estate wanted to use the statements in subsequent litigation against Mr Berezovsky. Justice Mann held that as the statements had been disclosed by Mr Berezovsky's solicitors without any express limitation on their use, it was not open to Mr Berezovksy to prevent their use by the estate against him. The Court of Appeal disagreed. Lord Neuberger MR said that the statements were obviously intended to remain confidential and were disclosed for a limited and defined purpose. In explaining the nature of limited waiver and its scope, Lord Neuberger noted:

> *[W]here privilege is waived, the question whether the waiver was limited, and, if so, the parameters of the limitation, must be determined by reference to all the circumstances of the alleged waiver, and, in particular, what was*

237 *Gotha City v. Sotheby's* [1998] 1 WLR 114; *Nederlandse Reassurantie Groep Holding NV v. Bacon & Woodrow and others* [1995] 1 All ER 976; *USP Strategies plc v. London General Holdings* [2004] EWHC 373.

238 *B v. Auckland District Law Society* [2003] 2 AC 736.

239 ibid., para. 68.

240 *Berezovsky v. Hine* [2011] EWCA Civ 1089.

© Law Business Research 2021

> *expressly or impliedly communicated between the person sending, and the person receiving, the documents in question, and what they must or ought reasonably have understood*[241]

The limited waiver principle was also applied in *CITIC Pacific Ltd v. Secretary for Justice*.[242] The Hong Kong Court of Appeal held that privilege had been waived in favour of the SFC for the purpose of its investigation only, even though at the time of the surrender of the documents to the SFC, CITIC's solicitors provided no written document setting out specific terms as to limitation of the waiver of privilege. It was only several weeks later, in response to an enquiry from the SFC, that CITIC stated in writing what it considered the terms of limitation to have been.

Another instance of the application of the limited waiver doctrine in the regulatory context is the *Property Alliance Group Ltd v. Royal Bank of Scotland plc* decision.[243] RBS claimed privilege over six documents that it had shown to various regulators and the DOJ and the Attorneys General of several US states. PAG argued that by showing those documents to third parties RBS had waived any privilege in them. The judge disagreed on the basis that the privilege had been waived for a limited purpose only (applying *B v. Auckland District Law Society* and *Berezovsky v. Hine*). Significantly, the judge held that the existence of 'non-waiver' agreements between RBS and the third parties – which recognised by certain 'carve-outs' that the regulator could use the information in a way which could in future destroy the privilege, for example, by publishing the material – did not undermine the limited nature of the waiver. Confidentiality and privilege would continue to be preserved unless some act such as publication, which would destroy the privilege, occurred.[244]

However, while under English law voluntary disclosure to a regulator may not entail a general waiver of privilege, this may be inconsistent with the position in other common law jurisdictions.[245]

In the case of *Dechert v. ENRC*,[246] the Court of Appeal held that the respondent, ENRC, was entitled to have proceedings for the detailed assessment of the bills of its former solicitors, Dechert, held in private and that ENRC had not waived privilege by commencing assessment proceedings. The implied waiver of privilege the application for detailed assessment had entailed was limited, temporary and extended only to the opposing party and to the judge. Lord Justice Gloster remarked that 'the concept of limited waiver is of general application, designed to ensure that the loss of LPP [legal professional

241 ibid., para. 29.

242 [2012] 2 HKLRD 701, discussed at Section 36.7.1.

243 [2015] EWHC 1557 (Ch).

244 ibid., para. 113.

245 CJQ 324, Case Comment by James Hayton.

246 [2016] 3 Costs LO 327.

© Law Business Research 2021

privilege] (given its fundamental importance) is limited to that which is necessary to protect other interests'.[247]

However, while it is clear from the authorities referred to above that the limits of a limited waiver will, in principle, be respected, parties providing documents to a regulator or investigator under a limited waiver may expose themselves to the possibility of a further, unintended waiver depending on how those documents are used. This issue arose in *PCP Capital Partners LLP v. Barclays Bank Plc*.[248] In that case, Barclays had provided documents to the SFO, in the context of a criminal investigation into the conduct of Barclays and others, under a limited waiver of privilege. The terms of the limited waiver permitted the SFO to use the documents in subsequent criminal prosecutions. The SFO did subsequently deploy those documents in criminal proceedings against a number of individuals (but not against Barclays itself, as the prosecution of Barclays had been discontinued by that time). The documents deployed in open court in those criminal proceedings lost confidentiality and thereby privilege. PCP obtained permission to use those formerly privileged documents in civil proceedings against Barclays. Barclays also relied on those documents (referred to in the civil proceedings as the 'Open Documents') in its witness statements in the civil proceedings. PCP argued that Barclays' reliance on the Open Documents gave rise to a collateral waiver of privilege in other documents with related subject matter. Barclays argued that there could be no collateral waiver because the Open Documents, when relied on in the civil proceedings, were not privileged (having lost privilege in the separate criminal proceedings when deployed by the SFO). There had therefore been no primary waiver to give rise to even a possibility of collateral waiver. The judge rejected that submission, finding: 'Barclays gave a limited waiver in the full knowledge that some or all would see the light of day at trial. So it can hardly be said that Barclays had nothing to do with the deployment of the Open Documents. In the circumstances of what happened, its original disclosure under the limited waiver was the starting point for what follows.'

If this is right (and, in the authors' view, there is considerable doubt about this), it means that a party providing privileged material to a regulator takes the risk that, if those documents subsequently lose confidentiality as a result of their use for a permitted purpose by the regulator (e.g., deployment in criminal proceedings), they will be available for use by a third party in subsequent civil litigation, but the former privilege holder will be unable to rely on those documents without risking a wider waiver of privilege.

Arguments may also arise as to the scope of any limited waiver and whether any wider waiver can be inferred from the conduct of the party waiving privilege or the circumstances in which privilege was waived. The scope of the principle of inferred waiver was the subject of consideration by the Divisional

247 ibid., para. 52.

248 [2020] EWHC 1393 (Comm).

© Law Business Research 2021

Court in *Belhaj v DPP*.[249] *Belhaj* concerned a judicial review of a decision by the Director of Public Prosecutions (DPP) not to prosecute a particular individual. While considering whether to prosecute, privileged material was passed by the government to the Metropolitan Police Service, the Crown Prosecution Service and the DPP under an express limited waiver of privilege. The claimants argued that the waiver must be taken to have extended not only to the police investigation and the decision whether to charge the relevant individual but also to any judicial review proceedings challenging that decision. The Divisional Court rejected that argument, finding that no such wider waiver could be inferred because there was no inevitable or necessary nexus between the decision of the DPP and the subsequent judicial review of the ultimate decision. The key question was whether these were discrete or composite processes. The Court found that the processes were discrete; waiver could not therefore be inferred. There remains scope for argument, on different facts, as to the extent to which a limited waiver to one person may be inferred to extend to another where that other person requires the relevant document for a purpose that is sufficiently connected to the purpose of the initial limited waiver.[250]

36.8.2 Collateral waiver

In certain circumstances the loss of privilege in a document can lead to waiver of privilege in other material. The rationale for this is one of fairness; the court is concerned to avoid having an incomplete picture of the events in question and to avoid 'cherry-picking' of privileged documents by a party.[251] Lord Bingham CJ commented in *Paragon Finance v. Freshfields* that: 'While there is no rule that a party who waives privilege in relation to one communication is taken to waive privilege in relation to all, a party may not waive privilege in such a partial and selective manner that unfairness or misunderstanding may result.'[252] For this reason it will be more difficult to establish collateral waiver where the initial disclosure was made inadvertently.

The weight of authority suggests that some reliance must be placed on the primary material before any waiver in collateral material can be triggered (although, as discussed above, in the *PCP* case it was held that the primary material in this context could be formerly privileged documents that had lost confidentiality, and thereby privilege, in separate proceedings). Simple disclosure and inspection of the primary material is probably insufficient. The

249 [2018] EWHC 513 (Admin).

250 See, in this regard, *Scottish Lion Insurance v. Goodrich Corporation* [2001] CSUH 18 and *FRC v. Sports Direct International Plc* [2019] 2 All ER 974, paras. 43 to 56.

251 *Nea Karteria Maritime Co v. Atlantic & Great Lakes Steamship Corporation (No. 2)* [1981] Com LR 138; *Paragon Finance v. Freshfields* [1999] 1 WLR 1183; *PCP Capital Partners LLP v. Barclays Bank Plc* [2020] EWHC 1393 (Comm).

252 [1999] 1 WLR 1183, 1188.

© Law Business Research 2021

necessary reliance has been said to be deployment of the primary material in court[253] but the approach of the courts to the question of what this means has not always been consistent.[254] Ultimately the touchstone is fairness, and waiver will be found where a party has crossed the line from, for example, merely referring to legal advice to actually relying on that advice in support of its position.[255] In *R v. Papachristos & Kerrison*,[256] an issue arose as to whether Innospec, a company that had pleaded guilty to corruption charges, had waived privilege in certain interview notes by providing a subsequent PowerPoint presentation to the SFO and the DOJ during negotiations, thereby waiving privilege in the presentation. Innospec was not a party to the proceedings and had not sought to deploy any document before the court. It was held that there had been no sufficient deployment by Innospec of the notes in the presentation to amount to a collateral waiver of privilege in respect of the notes as opposed to the PowerPoint presentation itself.

The court determined that there had been neither express nor collateral waiver in the interview notes because the waiver that had occurred over the PowerPoint was expressly limited and was in the context of the investigatory stage of the case.

In *PCP*, Justice Waksman analysed the relevant authorities and summarised the correct approach as being that 'first, the reference to the legal advice must be sufficient . . . and second, the party waiving must be relying on that reference in some way to support or advance his case on an issue that the court has to decide'.[257] As to the requirement that the reference to the legal advice must be 'sufficient', it was said that the distinction articulated in previous cases between reliance on the 'contents' of the legal advice (which would lead to a waiver) and reference to its 'effect' (which would not) cannot be applied mechanistically but that its application has to be viewed and made through the prism of (1) whether there is any reliance on the privileged material adverted

253 *Nea Karteria Maritime Co v. Atlantic & Great Lakes Steamship Corporation (No. 2)* [1981] Com LR 138; *General Accident Fire and Life Corp v. Tanter* [1984] 1 WLR 100.

254 Compare, for example, *MAC Hotels Limited v. Rider Levett Bucknall UK Limited* [2010] EWHC 767 (TCC) in which HHJ Havelock-Allan QC found that collateral waiver could occur by referring to and relying on privileged material in a witness statement served in support of an (as yet unheard) interlocutory application with the approach of Hobhouse J in *General Accident Fire and Life Corp v. Tanter* [1984] 1 WLR 100, holding that there was no collateral waiver where a privileged note of a conversation was used in cross-examination but before the author of the note was called and before it had been formally admitted in evidence.

255 *Mid-East Sales v. Engineering & Trading Co PVT Ltd* [2014] EWHC 892 (Comm); *PCP Capital Partners LLP v. Barclays Bank Plc* [2020] EWHC 1393 (Comm).

256 Unreported Southwark Crown Court, 13 May 2013.

257 *PCP Capital Partners LLP v. Barclays Bank Plc* [2020] EWHC 1393 (Comm), para. 48.

© Law Business Research 2021

to, (2) what the purpose of that reliance is and (3) the particular context of the case in question. This, the judge said, is an acutely fact-sensitive exercise.[258]

Reliance on part of a document may require disclosure of the whole. While severance may be possible if the document deals with entirely different subject matters, where the document deals with only one subject matter the court may conclude that it is or appears dangerous or misleading to allow a party to deploy part of the document and assert privilege over the remainder.[259]

Once privilege is waived in a particular document, the waiver extends to all documents relating to the same 'transaction', and possibly beyond.[260] The underlying principle applied by the courts is the need to ensure that the evidence adduced by the party claiming privilege is being presented fairly. Hence, in *R v. Secretary of State for Transport ex p Factortame Ltd*, Lord Justice Auld said:

> *In each case the question for the Court is whether the matters in issue in the document or documents in respect of which partial disclosure has been made are respectively severable so that the partial disclosed material clearly does not bear on matters in issue in respect of which material is withheld. The more confined the issue, for example as to the content of a single document or conversation, the more difficult it is likely to be to withhold, by severance, part of the document or other documents relevant to the document or conversations.*[261]

36.8.3 Inadvertent disclosure and restraining use of privileged documents

The Civil Procedure Rules (CPR) at rule 31.20 provide that, where a party inadvertently allows a privileged document to be inspected, the party who has inspected the document may use it or its contents only with the permission of the court. So, too, does Practice Direction 51U (PD 51U) – which provides a new pilot scheme[262] for disclosure in proceedings taking place in the Business and Property Courts, replacing Part 31 of the CPR except to the extent that its provisions are set out in PD 51U (at paragraph 19.1). While the solicitor for one side does not owe a duty of care to the other party,[263] where there is an obvious mistake (or, where PD 51U applies, where the solicitor has reason to suspect an inadvertent disclosure[264]), the solicitor should promptly notify the

258 ibid., para. 60. This approach was applied by Mrs Justice Moulder in *Tatneft v. Bogolyubov* [2021] 1 WLR 1612, where the judge rejected the suggestion that a reference to the subject matter of a communication will never be viewed as a waiver of privilege; nor can one say that a waiver in those circumstances would be 'most unlikely': para. 28.

259 *Great Atlantic v. Home Insurance* [1981] 1 WLR 529.

260 *Thanki*, paras. 5.129 to 5.133. See also *R (Jet2.com) v. Civil Aviation Authority* [2020] 2 WLR 1215, paras. 109 to 121 and *PCP Capital Partners LLP v. Barclays Bank Plc* [2020] EWHC 1393 (Comm), paras. 110 to 115.

261 (1997) 9 Admin LR 591, 599.

262 The pilot is due to run until at least 31 December 2022.

263 *Al-Fayed v. Commissioner of Police of the Metropolis* [2002] EWCA Civ 780, para. 16.

264 para. 19.2.

© Law Business Research 2021

other party and then, where the client wishes to use the document, make an application under rule 31.20 of the CPR (or paragraph 19 of PD 51U) to allow such use. Such use is unlikely to be allowed where the relevant party wishes to use the inadvertently disclosed document as the basis for a new claim, as distinct from the situation where a document is disclosed during litigation.[265]

The question of what is meant by an 'obvious mistake' was considered by the Court of Appeal in *Rawlinson & Hunter Trustees SA & Ors v. Director of the Serious Fraud Office*.[266] Lord Justice Moore-Bick stated that, once it is accepted that the person who inspected a document did not realise that it had been disclosed by mistake, despite being a qualified lawyer, it would be a strong thing for the judge to hold that the mistake was obvious. Further, given the scale of the disclosure in the case and the range of documents involved, general assertions in correspondence that the SFO did not intend to waive privilege were not sufficient to make it obvious that any document arguably privileged must have been disclosed by mistake. On the facts, it was held that it would not have been obvious that the documents at issue in the appeal had been disclosed by mistake. As noted above, the test in PD 51U for notification of an inadvertent disclosure is whether the solicitor has reason to suspect such disclosure. It seems likely that this will be interpreted as requiring a lower threshold than the standard of obvious mistake.

In *Ford v. FSA*,[267] the claimant established that he had joint interest privilege in two documents provided to the FSA by another party with the benefit of that privilege, and referred to by the FSA in a supplementary investigation report (SIR), without his consent. It followed that the FSA had not been entitled to rely on the content of the communications in the regulatory proceedings. The claimant subsequently sought relief including:

- the quashing of the warning notice issued by the FSA's Regulatory Decisions Committee that referred to the privileged material;
- the destruction of all copies of the privileged documents held by the FSA, together with their permanent deletion from databases and email accounts within the FSA;
- the destruction of all copies of the SIR and warning notices held by the FSA and their permanent deletion from databases and email accounts within the FSA, at least by redaction of the offending passages; and
- the redaction from all hard copy and electronic documents held by the FSA of quotations from or references to the substance of the privileged documents.

265 *Fadairo v. Suit Supply UK Lime Street Ltd* [2014] ICR D11 (EAT) (Singh J).

266 [2014] EWCA Civ 1129.

267 [2011] EWHC 2583 (Admin) (establishing that two of the documents referred to by the FSA in their supplementary investigation report were subject to joint interest privilege); [2012] EWHC 997 (Admin) (concerning the remedies sought by the claimant in relation to the use of the privileged documents by the FSA).

© Law Business Research 2021

Justice Burnett refused to quash the warning notice, in circumstances where he found that the privileged material formed a very modest part of the overall picture painted by a detailed exposition of the facts and matters on which the FSA relied; it was 'peripheral but not irrelevant'. Rather than equating the FSA's reliance on the privileged material with the public law concept of taking into account an irrelevant matter, the judge held that it was more accurate to consider the error as equivalent to a judicial or administrative body acting, in part, on inadmissible evidence. The warning notice, shorn of the offending references to privileged material, was said to remain a coherent, seamless and powerful document.

However, despite the FSA's submission that it would be sufficient to redact the privileged material from the SIR, warning notice and any other documents now to be deployed by the FSA, and to refrain from using or disseminating unredacted copies, Burnett J went further and ordered the FSA to use its best endeavours to identify and destroy such copies (both hard copy and electronic) of the privileged material that existed, together with such copies of the SIR and warning notices. In dealing with the claimant's further request for an order that anyone who had read the privileged documents or was aware of their content should be removed from further involvement in the relevant FSA investigation, the judge held that, while the approach identified in the private law context to the question whether a lawyer in possession of privileged material should be restrained from acting is a useful guide, when the question arises in judicial review proceedings there will necessarily be a public law element in the underlying dispute. The public interest may form an important element in any discretionary decision made in judicial review proceedings. In the particular circumstances of the case, he found that the order sought would be disproportionate and contrary to the public interest.

36.9 Maintaining privilege: practical issues

At the beginning of an investigation litigation may well not yet be in prospect (in which case litigation privilege will not apply) and therefore a corporate may wish to ensure that sensitive communications are, where possible, covered by legal advice privilege. It will be much more difficult to do this in light of the first-instance decisions in *The RBS Rights Issue Litigation* and *ENRC*, and a corporate embarking on an internal fact-finding investigation with a view to taking legal advice should therefore be aware of the risk that documents created pursuant to that investigation will be disclosable in any subsequent proceedings.

See Section 36.3.2.2

36.9.1 Conducting interviews

The conduct of interviews with potential witnesses is clearly an area of particular sensitivity. Because of the narrow view of who may constitute the 'client' in *Three Rivers No. 5*, as applied in *The RBS Rights Issue Litigation* and *ENRC* (which, while doubted by the Court of Appeal in both *ENRC* and *Jet2.com*, still remains the law), regulators or prosecutors may attempt to challenge a claim that the notes of evidence prepared by lawyers at such interviews

© Law Business Research 2021

are protected by legal advice privilege. In a speech to compliance professionals in March 2016, Alun Milford, then General Counsel of the SFO, emphasised the importance the SFO places on witness accounts of relevant events and stated, in this context:

> *1. We will view as uncooperative false or exaggerated claims of privilege, and we are prepared to litigate over them: to do otherwise would be to fail in our duty to investigate crime.*
> *2. If a company's assertion of privilege is well-made out, then we will not hold that against the company: to do otherwise would be inconsistent with the substantive protection privilege offers. We will simply judge the question of cooperation in our normal way against our published criteria.*
> *3. By the same token if, notwithstanding the existence of a well-made-out claim to privilege, a company gives up the witness accounts we seek, then we will view that as a significant mark of co-operation: here again, to do otherwise would be inconsistent with the substantive protection privilege offers.*
> *4. For the same reason, we will view as a significant mark of cooperation a company's decision to structure its investigation in such a way as not to attract privilege claims over interviews of witnesses.*[268]

In the first edition of this book, it was suggested that, to preserve privilege when conducting interviews with potential witnesses, in the case of employees, where possible, they should be expressly authorised by the corporate to communicate with the lawyers for the purposes of receiving advice. Such practice would be consistent with the decision of the Singapore Court of Appeal in *Skandinaviska Enskilda Banken v. Asia Pacific Breweries* and would in principle have provided a reasonable ground for asserting privilege on the basis of that decision. The position is much more difficult in light of *The RBS Rights Issue Litigation* and *ENRC* decisions. Following those decisions, and pending any reconsideration of the issue by the Supreme Court, only documents recording communications between the client (i.e., those within the organisation who are authorised to seek advice from, or receive the advice of, the lawyers) and the lawyers will be protected by legal advice privilege. That said, it seems likely that a corporate entity may nevertheless soon seek to maintain legal advice privilege over interview notes (notwithstanding that such a claim to privilege would likely be successfully challenged at a first instance) with the benefit of the Court of Appeal's comments in *ENRC* and *Jet2.com* about the unworkability of a narrow definition of 'client' in the corporate context.[269] However, until such a challenge (and clarification from the Supreme Court), notes of interviews with other employees or ex-employees of the client organisation, whether taken by

268 Alun Milford, General Counsel, SFO, Speech at the European Compliance and Ethics Institute, Prague (29 Mar. 2016).

269 In such a case it would seem very likely that a leap-frog certificate would be granted to enable the issue to be determined by the Supreme Court, bypassing the Court of Appeal.

© Law Business Research 2021

employees or by the lawyers, will be potentially disclosable in any subsequent proceedings, unless they can be said to form part of the lawyers' working papers. As to that, the decisions in *The RBS Rights Issue Litigation* and, at first instance, *ENRC* suggest that it will be necessary to establish in evidence that the notes, if disclosed, would betray the tenor of the legal advice. It may therefore be tempting for the lawyers to ensure that any notes recording factual information obtained from employees and ex-employees are produced so that they contain the solicitor's commentary and advice and are not merely a recitation of facts provided by the interviewee. There is no guarantee, however, that a court would consider such documents to be privileged in their entirety, and it might only be possible to maintain a claim to privilege in respect of those parts of the documents that evidence legal advice.

See Section 36.4.2

Of course, all interviews conducted for the dominant purpose of anticipated litigation ought to attract litigation privilege.

See Section 36.4.3

Where a corporation under investigation provides oral summaries of otherwise privileged interviews to a regulator or prosecutor, it is likely that this would be held to amount to a limited waiver in respect of matters communicated to the regulator or prosecutor because the information is provided for the limited purpose of the investigation.

See Section 36.8.1

36.9.2 Ensuring that any waiver is limited

It is clearly very valuable for a regulated entity to be able to waive privilege vis-à-vis the regulator for a particular purpose (e.g., in connection with a specific investigation) but without waiving it more generally. As noted above in Section 36.8.1, in *ENRC v. Dechert* the Court of Appeal has confirmed that the concept of limited waiver is of general application, designed to ensure that the loss of legal professional privilege (given its fundamental importance) is limited to that which is necessary to protect other interests.[270]

Although it may be possible for a regulated entity to contend that waiver of privilege was impliedly, if not expressly, limited (having regard to all the circumstances of the waiver), the safest course will always be to make clear at the time of disclosure that waiver is for a limited purpose only and confidentiality is otherwise being maintained.

However, as noted above, while it may be possible to achieve a limited waiver under English law, the waiver may not be so regarded in other jurisdictions. In addition, and as discussed above in the context of *PCP*, a party providing privileged documents to a regulator under a limited waiver of privilege should be aware that the permitted use of those documents by the regulator in subsequent proceedings may result in their loss of confidentiality and the loss of privilege, which may, in due course, lead to their use by a third party in civil proceedings.

270 [2016] 1 WLR 4205, para. 52 (*per* Gloster LJ).

© Law Business Research 2021

Redaction of documents 36.9.3

Where only part or parts of a document are privileged, the appropriate procedure (assuming the privilege holder wishes to maintain privilege) is to disclose the document but redact the privileged parts. Disclosure of a redacted document will not give rise to a waiver of privilege in respect of the redacted parts.[271] Disclosure of a redacted document in this way should be distinguished from deployment of a redacted document in court. In the latter circumstance, reliance on the unprivileged part of a document may give rise to collateral waiver in respect of the privileged part, where both parts deal with the same subject matter.

See Section 36.2

Where there is a dispute as to the justification for a redaction, the court may inspect the relevant document. In civil proceedings, the court's power to inspect documents to resolve an application for specific disclosure is found in the CPR at rule 31.19(6) or, where applicable, at paragraph 14.3 of PD 51U. Previously, it had been held that an order for inspection by the court is usually regarded as a solution of last resort and should not be undertaken unless the court considers that there is credible evidence that those claiming privilege have either misunderstood their duty, or are not to be trusted with the decision, or there is no reasonably practical alternative.[272] A more recent Court of Appeal decision has suggested that the hurdle to be surmounted before inspection is ordered is not as stringent, holding that the Court has a general discretion to inspect documents, but that it should nevertheless be cautious before exercising that discretion.[273]

In the criminal context, if the prosecution is asserting public interest immunity in order not to disclose material, there is a defined route to follow under the Criminal Procedure and Investigations Act 1996 (CPIA 1996) and the Criminal Procedural Rules (CrimPR) at rule 15.3.

The ability of the defence to challenge the adequacy of prosecution disclosure is provided for under section 8 of the CPIA 1996 and rule 15.5 of the CrimPR, after service of the defence case statement. The court may order disclosure of further material if the defence can demonstrate that the prosecution has that material and is required to disclose it in accordance with the CPIA 1996. A criminal court also has inherent jurisdiction to ensure a fair trial and, in the event of a dispute over the justification for a redaction, a judge can always review the material if he or she considers it appropriate.

Substantiating a claim to privilege if challenged 36.9.4

If a claim to privilege is challenged by an investigating authority or regulator, and the matter comes before the court, it will be necessary for the party claiming privilege to provide evidence to substantiate its claim. The principles

271 *GE Capital Corporate Finance Group v. Bankers Trust Co* [1995] 1 WLR 172.

272 *West London Pipeline v. Total UK* [2008] 2 CLC 258, para. 86(4)(c).

273 *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652, para. 40.

© Law Business Research 2021

to be applied in assessing that evidence were set out by Justice Beatson in *West London Pipeline v. Total UK*.[274] The judge explained that an affidavit claiming privilege:

> *should be specific enough to show something of the deponent's analysis of the documents or, in the case of a claim to litigation privilege, the purpose for which they were created. It is desirable that they should refer to such contemporary material as it is possible to do so without making disclosure of the very matters that the claim for privilege is designed to protect.*[275]

While these principles are well established, their application may in some instances be controversial. In *ENRC* the first-instance court did not consider that the evidential burden has been satisfied.[276] In particular, Andrews J was unimpressed by the explanation that had been given as to why evidence had to be adduced in the form of a witness statement from ENRC's solicitors rather than in the form of direct evidence from individuals at ENRC responsible for giving instructions to their lawyers. (The explanation for this was that the senior officers and employees at ENRC were not willing to give evidence in circumstances where they were or might become suspects in the SFO's investigation, without assurances that the SFO would not pursue cross-examination of those witnesses in the proceedings or seek to refer to that evidence against that witness or against ENRC in any subsequent criminal proceedings. The SFO was unwilling to give any such assurances.) This approach seemed to prejudice a corporate claiming privilege in a criminal context given that necessarily the company can only give direct evidence through its directors and employees who may themselves be at risk of investigation and prosecution.

In rejecting ENRC's evidence, Andrews J was also influenced by what she perceived to be an absence of contemporaneous documents to support the claim. In particular, she commented that she had not been shown any records of discussions either at board level or within any group at ENRC that might have shed light on what ENRC contemplated, and why they contemplated

274 [2008] 2 CLC 258. Although note, as set out above, the Court of Appeal's disapproval in *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652 of Beatson J's approach to inspection.

275 ibid., para. 53. It was also noted (at paras. 65, 86) that an affidavit is generally to be treated as conclusive unless it appears that the deponent has mischaracterised documents or it is reasonably certain from the evidence before the court that it is incorrect or incomplete on material points.

276 Similarly, in *The RBS Rights Issue Litigation*, Hildyard J did not consider that the evidence adduced by RBS was sufficient to make good RBS's claim that the interview notes comprised the lawyers' working papers as the evidence amounted to no more than a 'conclusory assertion'. As in *ENRC*, it is not easy to see what further evidence RBS could have adduced in support of the contention that disclosure of the notes would betray the trend of legal advice, without revealing the very matters over which RBS was seeking to claim privilege.

© Law Business Research 2021

it.[277] She therefore considered that for the purposes of the claim to litigation privilege, ENRC had failed to establish a reasonable anticipation of litigation.

The Court of Appeal in *ENRC* was critical of this approach and of the judge's failure to have proper regard to the unchallenged evidence of ENRC (put forward primarily by its solicitor) and the contemporaneous documents.[278] Following this decision, it appears that a corporate claiming privilege will not be prejudiced if, in light of the risk of investigation and prosecution of the individual directors and employees who might otherwise give evidence, it is left with no real choice but to give evidence through its lawyers.

Furthermore, the Court of Appeal's decision in *ENRC* confirms the proper approach explained in *West London Pipeline*, namely that the evidence in a witness statement or affidavit should be accepted unless there is good reason (e.g., the existence of contradictory contemporaneous documents) to think that the evidence is incorrect.[279]

Use of independent counsel 36.9.5

Where there is a potential dispute concerning the application of privilege, it is reasonably common for independent counsel to be appointed to review the relevant documents. Such counsel would then be prevented from acting for either side of the relevant dispute. An appointment may be made by the court or can be made more informally by the parties themselves. This process is, for example, frequently adopted by the SFO, although parties should always ensure the genuine independence of any counsel appointed.

In *R (McKenzie) v. Director of the Serious Fraud Office*,[280] the court was required to consider the procedures adopted by the SFO for dealing with potentially privileged material embedded in electronic devices seized using statutory powers or produced in response to a notice. The applicant complained that the SFO procedure was unlawful in using in-house technical staff to conduct an electronic search of the content of seized devices by reference to search terms for the purpose of isolating potentially privileged material for subsequent review by independent counsel. It was argued that this initial exercise should be contracted out by the SFO to independent IT specialists, despite the SFO having detailed procedures in place to ensure, in so far as possible, that its investigators would not gain access to any potentially privileged material

277 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205, para. 46.

278 See, in particular, *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, paras. 92, 93.

279 For a recent example of the Court nevertheless finding that it should go behind a party's assertion of privilege, see *The State of Qatar v. Banque Havilland SA & another* [2021] EWHC 2172 (Comm). The Court commented at para. 160 that, in circumstances where a party and its lawyers 'are, effectively, judges in their own cause', it is important to 'scrutinise carefully how and whether the claim for privilege is made out'.

280 [2016] EWHC 102 (Admin).

© Law Business Research 2021

before it had been reviewed by independent counsel. The applicant contended that the involvement of in-house SFO IT specialists and the uploading of the digital material, including the potentially privileged material embedded within it, onto the SFO's digital review system unnecessarily exposed the person to whom privilege attached to an avoidable risk that privileged material may come to the knowledge of the SFO and be used to his disadvantage.

The applicant in *McKenzie* argued that the same approach should apply when an investigating body lawfully comes into possession of potentially privileged material as applies to a solicitor in relation to privileged material relating to a former client. The investigating body must satisfy the court with convincing evidence that there is no real risk of the privileged material being disclosed to an investigator. The court disagreed, finding that it would not be appropriate to apply the same reasoning to the relationship between a criminal investigating body and the subject of its investigation as applies in relation to a solicitor and former client. In the case of an investigating body, there is no fiduciary relationship and the body is exercising statutory powers for the public good in the investigation of suspected crime. It would therefore be imposing too onerous an obligation on the SFO to require it to demonstrate that there could be no real risk of the privileged material being read by anyone involved in the investigation; instead, the seizing authority has a duty to devise and operate a system to isolate potentially privileged material from bulk material lawfully in its possession that can reasonably be expected to ensure that such material will not be read by members of the investigative team before it has been reviewed by an independent lawyer to establish whether privilege exists. There should also be clear guidance in place so that, if an investigator does by mischance read privileged material, that fact is recorded and reported, the potential conflict recognised and steps taken to prevent privileged information being deployed in the investigation. On the facts, the SFO procedure was held to satisfy these requirements.

© Law Business Research 2021

37

Privilege: The US Perspective

Richard M Strassberg and Meghan K Spillane[1]

Privilege in law enforcement investigations **37.1**

Attorney–client privilege **37.1.1**

The attorney–client privilege is recognised in the United States as 'the oldest of the privileges for confidential communications known to the common law'.[2] It is viewed as serving a crucial function in 'encourag[ing] full and frank communication between attorneys and their clients' and thereby promoting 'the observance of law and administration of justice'.[3] The attorney–client privilege protects information shared between a lawyer and the client, where the information is (1) a communication, (2) made in confidence, (3) between a person who is, or is about to become, a client (4) and a lawyer (5) for the purpose of obtaining legal advice or assistance.[4] Attorney–client privileged communications may take many forms, from oral communications, to emails, to text messages, so long as each communication is undertaken in confidence for the purpose of seeking or rendering legal advice.[5] Once the privilege is created, the privilege continues, and may be invoked at any time (unless it has been waived

1 Richard M Strassberg and Meghan K Spillane are partners at Goodwin.

2 *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

3 Id. at 392.

4 See, e.g., *In re Richard, Inc.*, 68 F.3d 38, 39-40 (2d Cir. 1995).

5 See, e.g., *Haines v. Liggett Grp.*, 975 F.2d 81, 90 (3d Cir. 1992) (explaining that privilege extends to verbal statements, documents and tangible objects conveyed in confidence for the purpose of legal advice).

© Law Business Research 2021

or is otherwise subject to an exception), even following the termination of the attorney–client relationship or the death of the client.[6]

In *Upjohn Co. v. United States*,[7] the United States Supreme Court held that a company's attorney–client privilege extends to company counsel's communications with employees in certain prescribed circumstances.[8] Rather than providing a simple objective test, the *Upjohn* court instead established five factors to guide courts in determining whether the company's privilege should extend to counsel's communications with its employees:

- whether the communications were made by employees at the direction of superior officers of the company for the purpose of obtaining legal advice;
- whether the communications contained information necessary for counsel to render legal advice, which was not otherwise available from 'control group' management;
- whether the matters communicated were within the scope of the employee's corporate duties;
- whether the employee knew that the communications were for the purpose of the company obtaining legal advice; and
- whether the communications were ordered to be kept confidential by the employee's superiors, including that the communications were considered confidential at the time and kept confidential subsequent to the interview.[9]

When these elements are established, courts generally consider communications between company counsel and an employee to be within the scope of the company's attorney–client privilege.[10]

See Section 37.3.1

While the privilege provides broad protection for confidential communications among those within the attorney–client relationship, disclosing the contents of these communications to a third party outside the scope of the protection (such as a government agency) may result in a waiver of the applicable privilege.

See Section 37.4

6 David M Greenwald and Michele L Slachetka, Protecting Confidential Legal Information, Jenner & Block LLP 104 (2015), https://jenner.com/system/assets/assets/8948/original/2015Jenner_26BlockAttorney-clientPrivilegeHandbook.pdf (citing *United States v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358 (D. Mass. 1950); *Swidler & Berlin v. United States*, 524 U.S. 399, 405–06 (1998)).

7 449 U.S. 383 (1981).

8 Id.

9 Id. at 394–96. While the majority of jurisdictions have adopted *Upjohn*'s approach, some states employ other tests to determine if conversations with an employee are covered by the company's privilege. See, e.g., *Motorola, Inc. v. Lemko Corp.*, No. 08 C 5427, 2010 WL 2179170, at *1–2 (N.D. Ill. 1 Jun. 2010) (noting that Illinois continues to apply the control group test and assess privilege questions accordingly).

10 To ensure that the employee understands the purpose of the interview, the expectation of confidentiality, and the scope of the attorney–client privilege, company counsel typically begins each meeting with a company employee by providing a summary of these factors, known as an '*Upjohn* warning'.

© Law Business Research 2021

Crime-fraud exception

The attorney–client privilege does not offer an absolute protection for all of a lawyer's communications with the client. An important exclusion is the crime-fraud exception, which removes the protection of the attorney–client privilege for communications concerning contemplated or continuing illegal or fraudulent acts.[11]

After a party has invoked the attorney–client privilege, the party seeking to abrogate the privilege under this exception has the burden of making a *prima facie* case that (1) the client was committing or intending to commit a crime or fraud and (2) the attorney–client communications at issue were in furtherance of that alleged crime or fraud.[12] Significantly, for the exception to be applicable, the party need not show that the alleged crime or fraud was actually completed, only that the crime or fraud was the objective of the communication.[13] Further, the party need not show that the attorney was aware of the alleged fraud or misconduct. In fact, the attorney's knowledge or ignorance of the crime is irrelevant. Instead, courts look to the client's intent or objective in the subject communication.[14] As the Supreme Court stated in *Clark v. United States*: 'A client who consults an attorney for advice that will serve him in the commission of a fraud will have no help from the law. He must let the truth be told.'[15]

For example, in the case of *United States v. Gorski*,[16] a defendant was indicted for making fraudulent representations related to the ownership and control of his company when bidding on government contracts.[17] The government alleged that the defendant fraudulently represented that his business qualified

11 See, e.g., *United States v. Zolin*, 491 U.S. 554, 563 (1989) (explaining that the crime-fraud exception 'assure[s] that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime') (citation omitted); *Clark v. United States*, 289 U.S. 1, 15 (1933); *In re Antitrust Grand Jury*, 805 F.2d 155, 162 (6th Cir. 1986); *In re Grand Jury Subpoenas Duces Tecum*, 773 F.2d 204, 206 (8th Cir. 1985); *United States v. Horvath*, 731 F.2d 557, 562 (8th Cir. 1984).

12 See *In re Grand Jury Subpoena*, 223 F.3d 213, 217 (3d Cir. 2000); *In re Sealed Case*, 754 F.2d 395, 399 (D.C. Cir. 1985).

13 See *In re Grand Jury Subpoena Duces Tecum*, 731 F.2d 1032, 1039 (2d Cir. 1984).

14 See, e.g., *United States v. Weingold*, 69 Fed. Appx. 575, 578 (3d Cir. 2003) (noting that the privilege may be disregarded even if the lawyer is innocent in relation to the fraudulent scheme); *In re Grand Jury Proceedings*, 87 F.3d 377, 381-82 (9th Cir. 1996) ('it is the client's knowledge and intentions that are of paramount concern to the application of the crime-fraud exception; the attorney need know nothing about the client's ongoing or planned illicit activity'); *In re Sealed Case*, 754 F.2d at 402 ('an attorney's ignorance of his client's misconduct will not shelter that client from the consequences of his own wrongdoing'); Horvath, 731 F.2d at 562 ('Whether the attorney is ignorant of the client's purpose is irrelevant')

15 289 U.S. 15 (1933).

16 807 F.3d 451 (1st Cir. 2015).

17 Id. at 455–56.

© Law Business Research 2021

as a service-disabled veteran-owned small business entity[18] and also sought to restructure his company through backdated documents to give the appearance of compliance with ownership regulations.[19] In response to a government subpoena for access to communications between the defendant and his lawyer regarding the ownership and restructuring efforts, the trial court held an *in camera* review and *ex parte* hearing, and determined that the requested documents should be produced under the crime-fraud exception.[20] On appeal, the First Circuit upheld the trial court's ruling, finding that (1) the indictment provided a reasonable basis to believe that the defendant was engaged in criminal or fraudulent activity and (2) there was a reasonable basis to believe that the attorney–client communications 'were intended by the client to facilitate or conceal the criminal or fraudulent activity'.[21] In so ruling, the court specifically noted that the crime-fraud exception does not require – and therefore does not reflect – any finding on the ultimate question as to whether the defendant acted wrongfully, nor does it bear on the conduct or intent of the lawyers involved.[22]

The crime-fraud exception has also been found to apply because of an attorney's misconduct, even if the client is found to be innocent of any wrongdoing.[23] The exception does not apply to attorney–client communications that reflect the solicitation or provision of legal advice concerning crimes or frauds that occurred in the past; such attorney–client communications remain protected,[24] unless the communications are made for the purpose of covering up past misconduct or obstructing justice.[25] Attorney–client communications reflecting advice about the legality of a client's intended course of conduct are likewise protected as privileged.[26] Finally, communications where an attorney

18 By representing his company as being a service-disabled-veteran-owned small business, the defendant was awarded certain set-aside or sole source government contracts for which he would not have otherwise been eligible. See 13 C.F.R. §§ 125.8 to 125.10.

19 Id.

20 Id. at 456–57.

21 Id. at 460–61 (internal quotation marks omitted).

22 Id. at 462.

23 See *Drummond Co. v. Conrad & Scherer, LLP*, 885 F.3d 1324, 1338 (11th Cir. 2018) (applying a balancing test 'to weigh the client's interest in secrecy against the reasons for disclosure'; see also *Navient Sols., LLC v. Law Offices of Jeffrey Lohman*, 19-cv-461, 2020 WL 1917837, *6 (E.D. Va. 20 Apr. 2020) (finding that 'the crime-fraud exception can apply where, as here, the attorney alone purportedly committed a crime or fraud of which the client was a victim')).

24 See, e.g., *Zolin*, 491 U.S. at 562 (explaining that the crime-fraud exception applies 'where the desired advice refers not to prior wrongdoing, but to future wrongdoing') (citation omitted).

25 See, e.g., *In re Grand Jury Proceedings*, 102 F.3d 748, 751 (4th Cir. 1996) (noting that the crime-fraud exception includes 'concealment or cover-up of [the client's] criminal or fraudulent activities'); *United States v. Laurins*, 857 F.2d 529, 540 (9th Cir. 1988) ('Obstruction of justice is an offense serious enough to defeat the privilege').

26 If a client seeks advice from counsel about the legality of a course of conduct and then relies to his or her detriment on that advice in taking action later determined to be unlawful, the client may choose to assert an 'advice of counsel' defence to demonstrate a lack of wrongful

© Law Business Research 2021

dissuades or prevents the client from engaging in further illegal conduct are also protected; such communications are viewed as serving an important purpose in the administration of justice by promoting legal conduct.[27]

Attorney work-product 37.1.2

In the United States, the doctrine of 'attorney work-product' also protects from disclosure certain documents and other materials prepared in anticipation of litigation or for trial. Although such work-product is most commonly prepared by an attorney, work-product protection may extend to materials prepared in anticipation of litigation by third parties at the attorney's direction, including materials prepared by the client.[28] But while the work-product doctrine offers certain protections for an attorney's impressions, opinions and legal conclusions, such documents are not considered 'privileged' like attorney–client communications, but instead are afforded a qualified protection from discovery.[29]

In the seminal case of *Hickman v. Taylor*,[30] the United States Supreme Court formally recognised the attorney work-product doctrine, establishing the scope of the protection to include materials prepared in anticipation of litigation.[31] The *Hickman* court also qualified this work-product protection by finding that, upon a showing of good cause, an adversary could obtain discovery of

---

intent. The client generally must show (1) full disclosure of all material facts to the attorney before seeking advice and (2) actual reliance on counsel's advice in the good faith belief that the conduct was legal. See, e.g., *United States v. West*, 392 F. 3d 450, 457 (D.C. Cir. 2004). Invoking the 'advice of counsel' defence generally waives the attorney–client privilege protecting the underlying communications with counsel related to the advice, since the client is putting the contents of those communications at issue. See, e.g., *Chevron Corp. v. Pennzoil Co.*, 974 F.2d 1156, 1162-63 (9th Cir. 1992).

There are limits to the ability of an individual employee to assert the advice-of-counsel defence where the client is the company, rather than the individual. In the civil context, for example, if the corporation controls the privilege over the attorney advice at issue, at least one court has found that the company may refuse to waive that privilege on behalf of the individual employee, even if the disclosure would amount to a complete defence of the individual. See *United States v. Wells Fargo Bank, N.A.*, 132 F. Supp. 3d 558, 566 (S.D.N.Y. 2015). In the criminal context, however, there appears to be split authority as to whether an individual's right to present his defence may trump the company's interest in preserving the privilege. Compare *United States v. Grace*, 439 F. Supp.2d 1125, 1142 (D. Mont. 2006) (finding that such evidence may be 'of such probative and exculpatory value as to compel the admission of the evidence over [the company's] objection as the attorney–client privilege holder'), with *Wells Fargo Bank, N.A.*, 132 F. Supp 3d at 562–63 (suggesting that the Supreme Court's rejection of a 'balancing test' for attorney–client privilege in *Swidler & Berlin v. United States*, 524 U.S. 399 (1998), may extend to criminal cases as well).

27 See, e.g., *In re Grand Jury Investigation*, 772 N.E.2d 9, 21–22 (Mass. 2002).

28 *Hertzberg v. Veneman*, 273 F. Supp. 2d 67, 76 (D.D.C. 2003).

29 See Fed. R. Civ. P. 26(b)(3).

30 329 U.S. 495 (1947).

31 Id. at 511.

© Law Business Research 2021

documents containing 'factual work product'.[32] The Court recognised that substantially greater – if not absolute – work-product protection should be given to documents that reflect the attorney's legal theories, strategy, assessments and mental impressions (opinion work-product).[33]

In *United States v. Nobles*,[34] the Supreme Court extended the work-product doctrine beyond the scope of materials created by counsel, recognising that attorneys often rely on the assistance of investigators and other agents in preparation for trial. The Court found that it is 'necessary that the [attorney work-product] doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself'.[35] Following the Supreme Court's guidance in *Nobles*, work-product protection is understood to be extended to material prepared 'by or for [a] party's representative' as long as the agent is assisting in preparing for litigation and working at the direction of the attorney.[36]

The modern federal work-product doctrine is codified in Rule 26(b)(3) of the Federal Rules of Civil Procedure (the Federal Rules), and stands in line with the Supreme Court's guidance in *Hickman* and *Nobles*. In particular, Rule 26(b)(3) eliminates the distinction between attorney work-product and non-attorney work-product, focusing on whether the materials were prepared in anticipation of litigation or trial.[37] Further, Rule 26(b)(3) preserves work-product protections unless the party seeking discovery has a 'substantial need' for the materials in the preparation of the party's case and the party is unable without 'undue hardship' to obtain the 'substantial equivalent' of the materials by other means.[38]

While the attorney work-product doctrine offers a qualified protection for documents created in anticipation of litigation, disclosing the contents of such documents to a third party outside of the attorney–client relationship (such as a government agency) may result in a waiver of this protection.[39] In addition, courts will examine the temporal proximity of the investigation to the threatened litigation in determining whether the work-product doctrine applies.[40]

See Section 37.4

32 Id. at 511–12.

33 Id. at 511 (noting that '[p]roper preparation of a client's case' involves creating such documents, and that providing them to opposing counsel on 'mere demand' would be 'demoralizing' to the legal profession and disserve both clients and the 'cause of justice').

34 422 U.S. 225, 238–39 (1975).

35 Id.

36 See Fed. R. Civ. P. 26(b)(3) advisory committee's note to 1970 amendment ('the weight of authority affords protection of the preparatory work of both lawyers and nonlawyers').

37 See Fed. R. Civ. P. 26(b)(3).

38 Id.

39 See *Qwest*, 450 F.3d at 1181, 1192.

40 See *Banneker Ventures, LLC v. Graham*, Civil Action No. 13-391 (RMC), 2017 WL 2124388, at *1–*2,*4–*5 (D.D.C. 16 May 2017) (finding that an internal investigation conducted 'over two years' after litigation was threatened was not conducted in anticipation of litigation and thus was not protected by the work-product doctrine).

© Law Business Research 2021

Common interest or joint defence privilege 37.1.3

The joint defence (or 'common interest') privilege is a doctrine that preserves the attorney–client privilege and work-product doctrine, despite disclosure of otherwise protected information to third parties.[41] As explained by the Second Circuit Court of Appeals, the privilege 'serves to protect the confidentiality of communications passing from one party to the attorney for another party where a joint defense effort or strategy has been decided upon and undertaken by the parties and their respective counsel'.[42] In general, a party asserting the privilege must demonstrate that (1) the communications were made in the course of a joint defence effort, (2) the statements were designed to further the effort and (3) the privilege has not otherwise been waived.[43] If the privilege is challenged, the burden is on the defendants to demonstrate the existence of a joint defence arrangement.[44]

While a joint defence arrangement has not been held to create a direct attorney–client relationship between counsel for one party and another, some courts have found that the sharing of confidential information creates an implied attorney–client relationship among the parties to the joint defence. In *United States v. Henke*,[45] for example, the Ninth Circuit held that the joint defence privilege can, in certain circumstances, create an implied attorney–client relationship, as well as a disqualifying conflict of interest. In that case, three executives – Gupta, Desaigoudar and Henke – were charged with conspiracy, making false statements, securities fraud and insider trading.[46] All three defendants participated in joint defence meetings where they shared confidential information.[47] On the eve of trial, however, Gupta entered into a co-operation agreement and agreed to testify for the government.[48] Gupta's lawyers threatened Desaigoudar and Henke's attorneys with legal action if they revealed any confidential information obtained as part of the joint defence meetings. Desaigoudar and Henke's attorneys eventually moved to withdraw because they believed their duty of confidentiality to Gupta prevented them from effectively cross-examining him.[49] The Ninth Circuit held that the lower court erred in denying the motions to withdraw, as the joint defence privilege

41 See *United States v. Schwimmer*, 892 F.2d 237, 243-44 (2d Cir. 1989), cert. denied, 502 U.S. 810 (1991).

42 Id.

43 See, e.g., *United States v. Bay State Ambulance*, 874 F.2d 20, 28 (1st Cir. 1989); *In re Bevill, Bresler & Schulman Asset Mgmt. Corp.*, 805 F.2d 120, 126 (3d Cir. 1986); *In re Grand Jury Subpoena Duces Tecum*, 406 F. Supp. 381, 385 (S.D.N.Y. 1975).

44 See *United States v. Weissman*, 195 F.3d 96, 100 (2d Cir. 1999).

45 222 F.3d 633 (9th Cir. 2000).

46 Id. at 635.

47 Id. at 637.

48 Id.

49 Id. at 637–38.

© Law Business Research 2021

created 'a disqualifying conflict where information gained in confidence by an attorney [became] an issue'.[50]

To mitigate the risk that information shared in the context of a joint defence agreement may lead to disqualification at a later time, many lawyers choose to include written disclaimers in their joint defence agreements along the following lines:

> *Nothing contained [in this agreement] shall be deemed to create an attorney–client relationship between any attorney and anyone other than the client of that attorney . . . and no attorney who has entered into this Agreement shall be disqualified from examining or cross-examining any joint defense participant who testifies at any proceeding, whether under a grant of immunity or otherwise, because of such an attorney's participation in this agreement, and it is herein represented that each party to this agreement has specifically advised his or her client of this clause.*[51]

Courts have found such provisions to permit an attorney to cross-examine a witness who was a former member of a joint defence arrangement and has since become a government co-operator, and have even permitted counsel to impeach the witness using statements that would otherwise be protected as privileged under the joint defence.[52]

The case of *SEC v. Rashid*[53] demonstrates the importance of both confirming and recording the intention to enter into a common interest relationship. In *Rashid*, the SEC was investigating the defendant's use of corporate expenses while employed at Apollo Management LP. During the investigation, the defendant retained counsel separate from that of the company, and eventually hired a separate firm to replace the first. During a later deposition of a representative from his prior law firm, the SEC sought to inquire about discussions with company counsel. When the defendant claimed such communications were protected by common interest privilege, the SEC moved to compel the testimony, arguing that the common interest privilege

50 Id. at 637.

51 See *Weissman*, 195 F.3d at 100.

52 See, e.g., *United States v. Almeida*, 341 F.3d 1318, 1326 (11th Cir. 2003) (holding that statements made under the joint defence doctrine 'do not get the benefit of the attorney–client privilege in the event that the co-defendant decides to testify on behalf of the government in exchange for a reduced sentence'); *United States v. Stepney*, 246 F. Supp. 2d 1069, 1086 (N.D. Cal. 2003) (finding that when a former co-defendant testified on behalf of the government, the joint defence team could cross-examine him on statements made pursuant to a joint defence agreement that (1) specified that the agreement would not create a duty of loyalty or an attorney–client relationship and (2) explicitly permitted the lawyer to use any material or information provided by the testifying defendant during the course of the joint defence in later cross-examining the witness.)

53 17-cv-8223, 2018 WL 6573451 (PKC) (S.D.N.Y. 13 Dec. 2018).

© Law Business Research 2021

is narrowly constructed and that the defendant did not meet his burden of showing that such a relationship existed. The court ordered the deposition to proceed, finding insufficient evidence of a common interest relationship. In so ruling, the court considered, among other things, (1) the lack of a written common interest agreement; (2) testimony from company counsel that they did not recall entering into a common interest relationship; (3) the defendants' lack of ability to recall specific details of the terms of the alleged agreement; and (4) that company counsel had delivered the *Upjohn* warnings at their first meeting with the defendant. The court determined that the common interest privilege cannot apply in a circumstance where there is no evidence that both parties agreed to pursue a joint legal strategy.

Further, to preserve the attorney–client privilege in the context of a joint defence arrangement, confidentiality must still be maintained against those outside the arrangement, because disclosure to a single outsider could constitute waiver of the information discussed in the outsider's presence.

Identifying the client 37.2

The 'client' in an attorney–client relationship is generally defined as the intended and immediate beneficiary of the lawyer's services, who communicates with the attorney to obtain legal advice, and interacts with the attorney to advance his or her own interests.[54] Defining the 'client' becomes more difficult in the context of corporate representation, as a company typically speaks by and through its employees, but the corporation's counsel represents not those individual agents, but rather the corporation itself.[55] As a general matter, a corporation's attorney–client privilege is controlled by the management of the organisation.[56] An employee or officer cannot assert the corporation's privilege if the corporation waives it,[57] and an employee cannot waive the corporation's privilege if the corporation asserts it.[58]

In cases where the interests of an employee are or may become adverse to that of the company during a government investigation, the Rules of Professional Conduct[59] dictate that attorneys explain clearly whom they repre-

54 Greenwald and Slachetka (supra note 6), at 15–16 (citing *Wylie v. Marley Co.*, 891 F.2d 1463 (10th Cir. 1989)).

55 See, e.g., *Judson Atkinson Candies, Inc. v. Latini-Hohberger Dhimantec, Inc.*, 529 F.3d 371, 389 n. 4 (7th Cir. 2008).

56 See *Commodity Futures Trading Comm'n v. Weintraub*, 471 U.S. 343, 348 (1985) (noting that 'the power to waive the corporate attorney–client privilege rests with the corporation's management').

57 See *In re Bevill*, 805 F.2d at 124–25; *In re Hechinger Inv. Co.*, 285 B.R. 601, 606 (D. Del. 2002) (finding that former officers and employees could not assert the corporation's privilege).

58 See *In re Grand Jury Proceedings*, 219 F.3d 175, 184 (2d Cir. 2000).

59 American Bar Association (ABA), Center for Professional Responsibility, Model Rules of Professional Conduct (2016), http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html.

© Law Business Research 2021

sent.[60] Interviewing employees in the context of a government investigation inevitably creates situations in which conflict between company and employee may arise. In particular, individuals should be advised to obtain separate counsel in situations where they are (1) the target of the investigation, (2) a probable whistleblower or (3) an employee facing risk of criminal liability. In any of these circumstances, employees should not be involved in the day-to-day supervision of company counsel's own investigation, including serving in the reporting chain.

Company counsel may encounter circumstances where an employee seeks to assert the attorney–client privilege to prevent the disclosure of information uncovered by counsel during investigative interviews by arguing that company counsel represents the employee as an individual. The Third Circuit in *In re Bevill Bresler & Schulman Asset Management Corp*, developed a five-part test (the *Bevill* test) to examine the merits of such an assertion by an individual employee against company counsel.[61] Under this test, employees must show that:

- they approached corporate counsel for the purpose of seeking legal advice;
- they made it clear that they were seeking advice in their individual capacity;
- counsel sought to communicate with the employee in this individual capacity, mindful of the conflicts with its representation of the company;
- the communications were confidential; and
- the communications did not concern the employee's official duties or the general affairs of the company.[62]

The *Bevill* test has been recognised by other jurisdictions as a means of assessing whether a company employee may assert attorney–client privilege in an individual capacity arising out of communications with corporate counsel.[63]

See Chapter 14 on employee rights

In *United States v. Blumberg*,[64] for example, the District of New Jersey applied the *Bevill* test where an individual employee sought to claim personal privilege protection for communications with the company's lawyer. In assessing the fifth factor of the test, the court considered the individual employee's claim that he had discussed with company counsel his 'potential for criminal exposure' and the fact that he was just a 'fact witness'.[65] The court ultimately concluded that this exchange did not create an individual attorney–client relationship, and that the company still owned the privilege covering the employee's communications, and thus could waive it (presumably over his objection).[66]

60 ABA Model Rule of Professional Conduct 1.13(f).

61 805 F.2d 120, 123, 125 (3rd Cir. 1986).

62 Id.

63 See, e.g., *United States v. Int'l Bhd. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am.*, AFL-CIO, 119 F.3d 210, 215 (2d Cir. 1997).

64 2017 U.S. Dist. LEXIS 47298 (D.N.J. 27 Mar. 2017).

65 Id. at *14.

66 Id. at *14–15.

© Law Business Research 2021

In *United States v. Holmes*,[67] the Northern District of California applied the Ninth Circuit's *Graf* test[68] to former Theranos chief executive officer Elizabeth Holmes's claim that her communications with company counsel were privileged, arguing that the firm represented both Theranos and also Holmes individually. The court found that Holmes's claim of privilege failed under the second, fourth and fifth prongs of *Graf* because there was no documentation to support the position that Holmes sought legal advice from counsel in her personal capacity (including engagement letters or evidence of fees paid) and her subjective belief was insufficient; there were no discussions between Holmes and counsel individually, but instead always in the presence of a third party; and all conversations with counsel related to Holmes's official duties and the general affairs of the company, rather than her individual interests. The court therefore held that company counsel did not represent Holmes in her individual capacity, and therefore she was not entitled to shield the communications from disclosure.

To mitigate the risks created by potentially divergent interests between the company and individual employees, counsel should be clear in their engagement letter about not only whom they represent, but also whom they do not. Further, mindful of the considerations outlined by the *Bevill* court, company counsel should take care during interviews with individual employees to limit their discussions to matters within the scope of the employee's official duties, rather than matters that may implicate the employee's personal interests. Finally, in the event that discussions with an individual employee diverge to matters implicating legal advice in the employee's individual capacity, counsel should reiterate to the employee that they have been retained to represent the company and the company's interests, and potentially advise the employee to retain separate counsel with respect to these other matters.

Maintaining privilege 37.3

Employee interviews 37.3.1

It is generally best if counsel conducts the employee interviews in the context of a government investigation, to ensure that what is said during the interview is covered by the attorney–client privilege, and that notes or memoranda documenting the interview are similarly privileged.[69] Recordings of interviews

67 *United States v. Holmes*, No. 118-cr-00258-EJD-1, 2021 WL 2309980 (N.D. Cal. 3 Jun. 2021).

68 *United States v. Graf*, 610 F.3d 1148, 1160–61 (9th Cir. 2010) (adopting the *Bevill* test and listing other jurisdictions who have adopted the test as well)

69 *Upjohn*, 449 U.S. at 394–99 (explaining that the attorney–client privilege protects attorney notes taken during interviews with employees during internal investigations); see also *In re Gen. Motors Ignition Switch Litig.*, 80 F. Supp. 3d 521, 527–28 (S.D.N.Y. 2015) (finding that documents relating to the internal investigation were protected from discovery because (1) the investigation was conducted at the direction of counsel, (2) those interviewed were told that the purpose of the interview was to facilitate the rendering of legal advice, (3) they were told that the content of the discussions should remain confidential, and (4) the communications underlying the published report were not shared with third parties).

© Law Business Research 2021

may, however, be considered purely factual communications that – as verbatim transcriptions – may not be subject to the attorney work-product doctrine.[70] Accordingly, it is general practice to have the attorney interviewer (or, more likely, another attorney in the room) take written notes of the interviews that include his or her thoughts and mental impressions. And because opinion work-product receives greater protection than fact work-product, it is more likely that written notes including an attorney's thoughts and impressions will be protected.[71]

While it is often most advantageous to have counsel conduct the witness interviews in an investigation, a court may still find that interviews conducted by non-lawyers maintain attorney–client privilege if they are acting as agents for lawyers. For example, in *In re Kellogg Brown & Root Inc* (*KBR*),[72] the DC Circuit court held that the work of an engineering and construction firm involved in an the internal investigation was afforded work-product protection where the investigation was conducted 'under the auspices of KBR's in-house legal department, acting in its legal capacity'.[73] The court held that '[s]o long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, the attorney–client privilege applies'.[74] The court's decision in *KBR* underscores the importance of making it clear that witness interviews conducted in the context of an internal investigation are for the purpose of rendering legal advice.[75]

Consistent with these principles, at the outset of any employee interview, counsel should give the employee an *Upjohn* warning, which makes clear that the communications between company counsel and the employees are confidential and protected as attorney–client privileged, and specifies that the privilege belongs to the company, and the company may choose to waive that privilege in the future. If clearly given, an *Upjohn* warning sets the boundaries of the interview and removes any doubt about whether counsel represents the employee.

---

70 See Fed. R. Crim. P. 26.2(a), (f)(2); see also *United States v. Nobles*, 422 U.S. 225, 230–32 (1975).

71 It is critical for counsel to establish the expectation of confidentiality and attorney–client privilege protection at the outset of each interview, as interview memoranda merely labelled as privileged and confidential will not 'retroactively render the earlier, otherwise-unprivileged discussions subject to the attorney–client privilege'. See *Erickson v. Hocking Technical College*, Case No. 2:17-cv-360, 2018 U.S. Dist. LEXIS 50075, at *6, *8 (S.D. Ohio 27 Mar. 2018).

72 756 F.3d 754 (D.C. Cir. 2014).

73 *KBR*, 756 F.3d at 757 (citing *Upjohn*, 449 U.S. 383).

74 Id. at 758–59.

75 In contrast, in *Wultz v. Bank of China*, the Southern District of New York granted a motion to compel documents collected by non-lawyers in the context of an internal investigation, where the party invoking the privilege failed to demonstrate that the documents were collected at the direction of an attorney to assist the attorney in providing legal advice. 304 F.R.D. 384, 395–97 (S.D.N.Y. 2015). The court also found that the work-product doctrine would not protect the documents from disclosure because the bank had failed to show that the documents would not have been created in 'essentially similar form irrespective of the litigation.' Id. at 395.

© Law Business Research 2021

In *KBR*, the DC Circuit noted that there are no 'magic words' that must be used to deliver a proper *Upjohn* warning.[76] Nevertheless, in practice, *Upjohn* warnings typically include some variation of the following components:

- *The lawyer represents the company only and not the witness personally.*
- *The lawyer is collecting facts for the purpose of providing legal advice to the company.*
- *The communication is protected by attorney–client privilege, which belongs exclusively to the company, not the witness.*
- *The company may choose to waive the privilege and disclose the communication to a third party, including the government.*
- *The communication must be kept confidential, meaning that it cannot be disclosed to any third party other than the witness's counsel.*[77]

Once the *Upjohn* warning is given, and before any substantive interview commences, counsel should confirm that the witness understands the warning, answer any questions the witness has about it and establish that the witness is agreeable to being interviewed under these terms. As an additional precaution, counsel should remind the witness at the conclusion of the interview not to discuss the substance of the interview with anyone else, except to the extent that the witness wishes to convey additional information or to ask follow-up questions of counsel.

Once a witness interview is complete, memorialising the content of the interview is essential to the investigation. The summary should state expressly that it does not constitute a verbatim transcription of the interview and that the summary contains the thoughts, mental impressions and legal conclusions of counsel. The summary should also confirm the delivery of the *Upjohn* warning, indicating the employee's understanding of the warning and willingness to proceed with the interview.

The importance of recording the provision of the *Upjohn* warning is underscored by the case of *United States v. Ruehle*.[78] In *Ruehle*, outside counsel conducted an interview of an employee, William J Ruehle, during an internal investigation. During the interview, Ruehle made statements that he later sought to suppress from his criminal trial. He argued that the statements were privileged because outside counsel had previously represented him in his individual capacity in a shareholder lawsuit, and counsel had not otherwise advised him that his statements during the internal investigation could be disclosed to third parties. The court found there to be inadequate evidence that Ruehle had been given *Upjohn* warnings, finding it persuasive that there was no reference to the delivery of *Upjohn* warnings in counsel's interview memoranda. While

76 *KBR*, 756 F.3d at 758.

77 See, e.g., ABA, White Collar Working Group, *Upjohn Warnings: Recommended Best Practices When Corporate Counsel Interacts With Corporate Employees* (17 Jul. 2009).

78 583 F.3d 600 (9th Cir. 2009).

© Law Business Research 2021

See Chapters 8 on witness interviews and 14 on employee rights

the court's decision was later reversed on other grounds, this case illustrates the importance of maintaining a record of the delivery of *Upjohn* warnings. The absence of an *Upjohn* warning is not dispositive, however, as courts will also consider whether the employee and attorney 'explicitly or by their conduct manifest[ed] an intention to create an attorney/client relationship'.[79] Without an *Upjohn* warning, courts will assess whether the attorney had 'reason to suspect that the firm's interests and the [employee's] interests diverged' during the period in question and also whether the employee's 'assumption' that the Company attorney was his personal attorney was 'reasonable' for someone of his knowledge and experience.[80]

Issues may also arise when interviewing current employees in the context of an internal investigation, to the extent that the investigation is prompted by a government inquiry when there is extensive coordination with a government regulator. In *United States v. Connolly*,[81] a bank engaged outside counsel to conduct an investigation into the bank's LIBOR practices that was prompted by a letter from the Commodity Futures Trading Commission (CFTC) requesting that the bank 'cooperate fully' by 'voluntarily engaging' outside counsel to conduct a review. During the investigation, outside counsel 'coordinated extensively' with both the CFTC and the Department of Justice (DOJ), and the government agencies gave substantial direction to the lawyers as to which employees should be interviewed and how to approach the interviews. After a bank employee, Connolly, was later indicted and convicted for conspiracy and wire fraud for his conduct in connection with the manipulation of LIBOR, he moved to vacate his conviction on the theory that his prosecution was predicated on, and fatally tainted by, statements that he gave in interviews conducted by outside counsel during the investigation. He argued that counsel was effectively deputised by the government in conducting the interviews, and as a result his statements should be deemed involuntary and rendered inadmissible under *Garrity v. New Jersey*,[82] since he made the statements under the threat of termination of employment in violation of his Fifth Amendment rights. Chief Judge Colleen McMahon of the Southern District of New York found that outside counsel here was '*de facto* that Government for *Garrity* purposes' and noted that she was 'deeply troubled by this issue', which had 'profound implications' for how government investigations are conducted. And while the Court ultimately declined to overturn the employee's conviction, holding that the government did not 'use' his compelled statements in indicting or prosecuting him, the Court's comments and admonition will undoubtedly have a significant impact on the level of coordination with government agencies in investigations going forward.

See Chapter 10 on co-operating with authorities

79 *See In re Grand Jury Investigation*, No. 19-15, 2019 WL 217916, *13 (D. D.C. 4 Mar. 2019).

80 Id. at *16 (finding that a sophisticated attorney would have no need for an *Upjohn* warning to understand that company counsel was not his personal attorney).

81 No. 16-Cr-00370, 2019 WL 2120523 (S.D.N.Y. 2 May 2019).

82 385 U.S. 493 (1967).

© Law Business Research 2021

Former employees 37.3.2

Interviews with former corporate employees about matters within the scope of their prior employment may also be protected by the attorney–client privilege.[83] Indeed, while courts of different jurisdictions are split as to whether attorney–client privilege should extend to discussions with former employees as a general matter,[84] most courts agree that narrowly tailored discussions related to the period of the individual's former employment should remain privileged.[85] Consequently, counsel conducting an investigation should carefully focus the interview with a former employee on matters that occurred during the former employee's tenure, as some district courts have held that interviews with a former employee on subjects that occurred after the employment had ended are not privileged.[86]

In determining whether a former employee is likely to be co-operative or to maintain the confidentiality of the interview, counsel should consider (1) the circumstances of the employee's departure and (2) whether the employee will be contractually obliged to maintain the confidentiality of the interview, through a severance agreement, for example.

Non-legal advice 37.3.3

At the outset of an internal investigation, the corporation should document that the investigation is being conducted for the purpose of obtaining legal advice and at the direction of counsel. If such intention is not documented, and it appears instead that employee interviews are being conducted in the

83 *Upjohn*, 449 U.S. at 403 (Burger, CJ, concurring) (finding a former employee's communication is privileged when the employee 'speaks at the direction of the management with an attorney regarding conduct or proposed conduct within the scope of employment').

84 Compare *In re Coordinated Pretrial Proceedings in Petroleum Prod. Antitrust Litig.*, 658 F.2d 1355, 1361 n. 7 (9th Cir. 1981) (finding that the *Upjohn* rationale extended the attorney–client privilege to former employees because 'former employees . . . may possess the relevant information needed by corporate counsel to advise the client with respect to actual or potential difficulties'), with *Clark Equip. Co. v. Lift Parts Mfg Co.*, No. 82 C 4585, 1985 WL 2917, at *5 (N.D. Ill. 1 Oct. 1985) (declining to apply privilege protection to communications with former employees, noting that '[i]t is virtually impossible to distinguish the position of a former employee from any other third party who might have pertinent information about one or more corporate parties to a lawsuit').

85 See, e.g., *United States ex rel. Hunt v. Merck-Medco Managed Care, LLC*, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004) ('the line to be drawn is not difficult: if the communication sought to be elicited relates to [the former employee's] conduct or knowledge *during* her employment . . . , or if it concerns conversations with corporate counsel that occurred *during* her employment, the communication is privileged; if not, the attorney–client privilege does not apply') (emphasis in original).

86 See, e.g., *United States ex rel. Hunt v. Merck-Medco Managed Care*, LLC, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004); *Peralta v. Cendant Corp.*, 190 F.R.D. 38, 41 (D. Conn. 1999). Interviews about such topics may, however, be covered by work-product protection.

© Law Business Research 2021

context of a non-legal investigation, such communications may not be effectively cloaked in the attorney–client privilege. In *Koumoulis v. Independent Financial Marketing Group Inc*,[87] for example, plaintiffs were former and current employees of a company in the business of providing investment products to financial institutions.[88] The Eastern District of New York found that reports documenting internal discrimination complaints and the subsequent investigation by the company's human resources managers were not protected as attorney–client privileged because 'their predominant purpose was to provide human resources and thus business advice, not legal advice'.[89]

In light of *Koumoulis*, counsel must be ever mindful of stating explicitly at the outset of an investigation that its communications are outside the course of the day-to-day operation of the client's business and are explicitly aimed at assisting the delivery of legal advice. To the extent that litigation is reasonably foreseeable, it should be noted in all memoranda generated in the context of the investigation. Further, counsel should confirm with individual employees that when they are seeking legal advice – rather than business advice – the employees should be similarly explicit in their communications, labelling them as 'attorney–client privileged'. More important than any label or transcription, however, is that the context of such documents must reflect the solicitation and receipt of legal, rather than business, advice.[90]

37.4 Waiving privilege

Even if all the prerequisites for establishing attorney–client privilege are met, whenever a client discloses confidential communications to third parties, including government agencies, the disclosure may constitute a waiver of the privilege as to both the communication that has been disclosed and other communications relating to the same subject matter. Federal Rule of Evidence 502(a) governs disclosures made to a federal officer or agency and also the scope of waiver in such disclosures.[91] The rule explicitly states that disclosures of attorney–client or work-product protection to the federal government creates a waiver that extends to other undisclosed communication or information in a federal or state proceeding if (1) the waiver is intentional,

87 295 F.R.D. 28 (E.D.N.Y. 1 Nov. 2013), aff'd in part, 29 F. Supp. 3d 142 (E.D.N.Y. 21 Jan. 2014).

88 Id. at 33.

89 Id. at 46. See also *Welland v. Trainer*, No. 00 Civ. 0738 (JSM), 2001 WL 1154666, at *2 (S.D.N.Y. 1 Oct. 2001) (finding certain communications between the investigator, who conducted the internal investigation, and in-house and outside counsel are protected by attorney–client privilege because the investigator received legal advice from counsel under circumstances in which the employee under investigation was an executive and litigation was expected if the employee were terminated).

90 *Koumoulis*, 29 F. Supp. 3d at 147 (finding that legal memoranda must contain more than 'a stray sentence or comment within an email chain referenc[ing] litigation strategy or advice').

91 Federal Rules of Evidence [Fed. R. Evid.], 502(a).

© Law Business Research 2021

(2) the disclosed and undisclosed communications or information concern the same subject matter and (3) they ought in fairness to be considered together.[92]

While the 'fairness' requirement of Rule 502(a) creates some uncertainty as to when subject-matter waiver might occur, in practice, courts typically look to the reason for the initial disclosure when determining the scope of a waiver. If a court determines that a party selectively disclosed privileged information to gain a strategic advantage to the government's detriment, it is more likely to find a full subject-matter waiver.[93] But, if the disclosure occurred outside the context of litigation, or if the disclosure was not intended for – or did not actually result in – a strategic advantage to the disclosing party, the court is likely to find a limited waiver.[94] In the case of *United States v. Treacy*,[95] for example, Judge Rakoff of the Southern District of New York quashed a defendant's subpoena for a law firm's interview memoranda that had not previously been provided to the government, rejecting the theory that furnishing some interview memoranda to the government waived privilege with regard to others covering the same subject matter.[96] The Court relied on the advisory committee notes in Rule 502(a) in support of its 'fairness' assessment, finding that subject-matter waiver should be reserved for the narrow circumstances where a party seeks to disadvantage their adversary through a selective or misleading disclosure.[97] Further, if a party chooses to disclose attorney work-product to the government – in the form of White Papers, presentations or other memoranda – with the purpose of dissuading the government from bringing suit, one court has held that such a disclosure will waive any privilege with respect to those materials, which may subsequently be discoverable by third parties.[98]

92 Id.

93 See, e.g., *In re Teleglobe Commc'ns Corp.*, 493 F.3d 345, 361 (3d Cir. 2007) ('[w]hen one party takes advantage of another by selectively disclosing otherwise privileged communications, courts broaden the waiver as necessary to eliminate the advantage')

94 See, e.g., *In re Keeper of the Records*, 348 F.3d 16, 24 (1st Cir. 2003) (holding that 'the extrajudicial disclosure of attorney–client communications, not thereafter used by the client to gain adversarial advantage in judicial proceedings, cannot work an implied waiver of all confidential communications on the same subject matter'); *Swift Spindrift, Ltd. v. Alvada Ins. Inc.*, No. 09 Civ. 9342 (AJN)(FM), 2013 WL 3815970, at *5 (S.D.N.Y. 24 Jul. 2013) (finding that the intentional disclosure of two privileged emails did not result in a broader waiver of the attorney–client privilege because (1) the emails were actually unfavourable to the disclosing party's position, and (2) therefore could not be used to the other parties' disadvantage).

95 No. S2 08 CR 366 (JSR), 2009 WL 812033 (S.D.N.Y. 24 Mar. 2009).

96 Id. at *1–2.

97 Id.

98 See *Alaska Electrical Pension Fund v. Bank of America Corp.*, 2017 WL 280816. at *2–3 (S.D.N.Y. 20 Jan. 2017); see also SEC Division of Enforcement, Enforcement Manual, Office of the Chief Counsel, § 3.2.3.2 (28 Oct. 2016) (specifying that White Papers, excluding Wells notices, submitted to the SEC may be discoverable by third parties in accordance with applicable law).

© Law Business Research 2021

37.4.1 Co-operation credit and waiver

Corporations subject to criminal or regulatory investigations have long faced the question of whether and when to turn over privileged material to the government. Waiving privilege has historically resulted in increased co-operation 'credit' from the DOJ[99] and the Securities and Exchange Commission (SEC).[100] However, changes to DOJ guidelines now forbid the government from requesting that companies waive attorney–client privilege, and preclude consideration of whether the corporation waived privilege in assessing co-operation credit.

Indeed, in response to pressure from the private sector and the legislative and judicial branches, on 12 December 2006, the then Deputy Attorney General Paul J McNulty issued a memorandum containing new corporate charging guidelines for federal prosecutors through a revision to the Principles of Federal Prosecution of Business Organizations.[101] The McNulty Memorandum required that, before requesting a waiver of attorney–client or work-product privileged information from a corporation under investigation, prosecutors must establish a 'legitimate need' for privileged communications and seek approval of the US Attorney, who must obtain written approval of the Deputy Attorney General.[102]

In 2008, the DOJ replaced these guidelines in a memorandum authored by the then Deputy Attorney General Mark R Filip.[103] The Filip Memorandum further adjusted what factors the government should consider in determining whether a corporation deserves 'co-operation credit': where co-operation credit had previously turned on factors including waiver of attorney–client privilege or work-product protections, it will now focus on disclosure of relevant facts.[104] In other words, a company could receive the same co-operation credit if it disclosed facts contained in non-privileged materials as it would if it disclosed

99 See, e.g., Memorandum from Larry D Thompson, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (20 Jan. 2003); see also Memorandum from Paul McNulty, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (12 Dec. 2006) (McNulty Memorandum).

100 See, e.g., Sec. & Exch. Comm'n, SEC Rel. No. 34-44969, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions (the Seaboard Report) (23 Oct. 2001) (explaining that a company that disclosed internal investigation interviews without asserting privilege had fully co-operated).

101 McNulty Memorandum (supra note 99).

102 Id. at 8–9.

103 Memorandum from Mark R Filip, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (28 Aug. 2008).

104 Id.

© Law Business Research 2021

facts contained in privileged materials, so long as the company discloses all relevant facts known to it.

In September 2015, the DOJ issued a memorandum authored by then Deputy Attorney General Sally Quillian Yates entitled 'Individual Accountability for Corporate Wrongdoing'.[105] The Yates Memorandum set forth policies intended to guide the DOJ in holding individual defendants civilly and criminally liable for corporate misconduct.[106] Significantly, the Yates Memorandum now requires a company to disclose 'all relevant facts relating to the individuals responsible for the misconduct' for the company 'to be eligible for any cooperation credit'.[107] While Yates has publicly remarked that these new policies are not intended to undermine the Filip Memorandum's guidance regarding the waiver of attorney–client privilege,[108] the mandate to disclose 'all relevant facts' creates some uncertainty as to whether, at least practically speaking, such a waiver may now be required once again. In describing the impact of the Yates Memorandum on companies seeking co-operation credit, Yates explained the DOJ's view that 'facts are not [privileged]', and therefore a company must 'produce all relevant facts – including the facts learned through . . . interviews [with company employees] – unless identical information has already been provided'.[109]

In November 2017, the DOJ adopted the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, which provided guidance regarding the credit that the DOJ might provide to companies who self-report FCPA violations. The policy authorises certain benefits – including a presumption that self-reporting companies will not be criminally charged – for companies that meet the DOJ's rigorous requirements of disclosure, co-operation and remediation, including disgorgement of ill-gotten gains.[110] In March 2018, the DOJ announced an expansion of the FCPA Corporate Enforcement Policy, noting that it may be employed as non-binding guidance in criminal cases beyond those arising under the FCPA. This announcement underscores the DOJ's encouragement of self-reporting and co-operation by companies in a wide range of criminal cases.

---

105 Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Individual Accountability for Corporate Wrongdoing (9 Sep. 2015) (Yates Memorandum).

106 Id. at 1.

107 Id. at 2.

108 Remarks of Deputy Att'y Gen. Sally Quillian Yates delivered at American Banking Association and American Bar Association Money Laundering Enforcement Conference (16 Nov. 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0 ('there is nothing in the new policy that requires companies to waive attorney–client privilege or in any way rolls back the protections that were built into the prior factors').

109 Id.

110 Corporate Enforcement Policy, U.S. Dep't of Justice, Justice Manual § 9-47.120 (2017), available at https://www.justice.gov/criminal-fraud/corporate-enforcement-policy.

© Law Business Research 2021

On 29 November 2018, Deputy Attorney General Rod J Rosenstein delivered remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act[111] that reaffirmed the central tenets of the Yates Memorandum, but also announced a revised policy that provides federal prosecutors with greater discretion concerning whether to pursue individuals, based on varying standards between civil and criminal investigations. In particular, Rosenstein stated that companies are no longer expected to 'admit the civil liability of every individual employee' to qualify for co-operation credit. Instead, companies should focus on identifying individuals who were 'substantially involved in or responsible for the misconduct', including members of senior management or the board of directors. While Rosenstein's comments have been considered as a reversion to pre-Yates priorities, where the 'primary goal' in civil cases is to recover money, recent court decisions have demonstrated a continued focus on the concepts of individual accountability articulated by Yates.[112]

On 28 October 2021, Deputy Attorney General Lisa Monaco delivered the keynote address at the ABA's 36th National Institute on White Collar Crime and announced, among other things, three actions that the DOJ plans to take with regard to its enforcement priorities. First, Monaco signalled that the DOJ is reverting to the co-operation requirements as previously outlined in the Yates Memorandum in 2015. In particular, Monaco reiterated the prior guidance (later loosened under the Trump administration) that in order to receive co-operation credit, organisations must provide to the DOJ 'all non-privileged information about individuals involved in or responsible for the misconduct at issue'. Second, Monaco announced that when evaluating a corporation's history of prior misconduct, 'all prior misconduct needs to be evaluated . . . , whether or not that misconduct is similar to the conduct at issue in a particular investigation'. Third, Monaco discussed the DOJ's imposition of corporate compliance monitors, emphasising that monitorships are not 'disfavored' or the 'exception to the rule' but rather an important tool to 'encourage and verify compliance'. Monaco stated that the DOJ will eliminate any perception of favouritism in the monitorship programme by studying how corporate monitors are chosen and how the processes can be standardised across divisions and offices.

In light of this guidance, corporate counsel must be mindful about entering into joint defence agreements that might limit their ability to share with the

111 See 'Deputy Attorney General Rod J Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act', Office of Public Affairs, U.S. Dep't of Justice (29 Nov. 2018) https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

112 See *United States ex rel. Doe v. Heart Solutions PC et al.*, 923 F.3d 308, 314-15 (3d Cir. 2019) (sustaining summary judgment against an individual defendant even though she had no financial stake in the corporation profiting from the fraud, citing the Yates Memorandum as endorsing enforcement under the false claims act against individuals 'at all levels' of the corporate structure).

© Law Business Research 2021

government the underlying facts learned during the investigation, especially if the company is facing exposure to a potentially devastating criminal charge if it does not receive credit for co-operating with the government. In addition, the Yates Memorandum underscores the importance of issuing comprehensive *Upjohn* warnings when interviewing company employees, as a mandate to disclose 'all relevant facts' may involve the revelation to the government of facts disclosed by (potentially culpable) employees in the context of investigative interviews.

Inadvertent disclosure of privileged material 37.4.2

Particularly in cases where large numbers of documents are produced, it is not uncommon that a party might inadvertently disclose privileged communications. Federal Rule of Evidence 502(b) governs the court's treatment of attorney–client privileged and work-product material that has been inadvertently disclosed. The rule provides that, when making a disclosure in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if '(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error'.[113] According to Rule 502(b)'s advisory committee explanatory notes, courts are to consider several factors in determining whether the privilege holder took steps to promptly rectify the error, including:

- the reasonableness of precautions taken;
- the time taken to rectify the error;
- the scope of discovery;
- the number of documents reviewed and the time constraints for production;
- the extent of disclosure' and
- 'the overriding issue of fairness'.[114]

The explanatory notes also suggest that a party can help demonstrate that its steps were reasonable by employing 'advanced analytical software applications and linguistic tools' in screening for privilege.[115]

Federal Rule of Civil Procedure 26(b)(5)(B) provides additional guidance on how clawback provisions may intersect with a claim of inadvertent disclosure. Under this rule, if information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, 'the party making the

113 Fed. R. Evid. 502(b).

114 Fed. R. Evid. 502 advisory committee's note.

115 Id.

© Law Business Research 2021

claim may notify any party that received the information of the claim and the basis for it'.[116] After being notified, a party:

> *must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim.*[117]

While the same clawback procedure is not explicitly contemplated in the criminal context, parties making disclosures in federal proceedings or to a federal office or agency may choose to enter into a voluntary clawback arrangement under Rule 502(e), including an explicit agreement that inadvertent disclosure will not constitute a waiver.[118] Such agreements are generally binding only on the parties to the agreement.[119] A carefully drawn clawback agreement can be to the benefit of everyone in the context of a government investigation: the agency will benefit from receiving discovery more expeditiously, and the producing party will benefit from minimising the risk and added review costs in the absence of such an agreement.[120] Even where counsel takes reasonable steps to prevent the disclosure of privileged material, the complexity of government investigations creates a real risk that such materials may still be inadvertently produced. To further mitigate this risk, document production letters should include unequivocal language, preserving the client's ability to claw back and recover inadvertently disclosed documents.

37.5 Selective waiver

The attempt to disclose privileged material to the government in the context of an investigation, while still claiming privilege and confidentiality over that same material as to other third parties, is called 'selective waiver'. Generally, courts have refused to sanction selective waiver, finding that the disclosure of privileged material to the government destroys the confidentiality necessary to maintain a claim of privilege in the first place, and therefore waives the privilege with respect to other third parties as well.[121]

---

116 Fed. R. Civ. P. 26(b)(5)(B).

117 Id.

118 Fed. R. Evid. 502(e).

119 Id.

120 In the context of an investigation that is already public, a party may choose to request a court order limiting the scope of waiver and/or setting forth a clawback procedure to govern its production. See Fed. R. Evid. 502(d).

121 See, e.g., *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289 (6th Cir. 2002); *United States v. Mass. Inst. of Tech.*, 129 F.3d 681 (1st Cir. 1997); *Westinghouse Elec. Corp. v. Republic of the Philippines*, 951 F.2d 1414 (3d Cir. 1991); *In re Martin Marietta Corp.*, 856 F.2d 619 (4th Cir. 1988); *Permian Corp. v. United States*, 665 F.2d 1214 (D.C. Cir. 1981).

© Law Business Research 2021

The leading case applying the selective-waiver analysis is *Diversified Industries Inc v. Meredith*.[122] In *Diversified Industries*, a corporation retained outside counsel to conduct an internal investigation into allegations of bribery.[123] The internal report prepared by outside counsel was then produced to the SEC.[124] The Eighth Circuit held that this disclosure constituted only a 'limited waiver' that did not preclude the corporation from subsequently withholding the report from private litigants on the grounds of attorney–client privilege.[125] The court reasoned that a contrary ruling may undermine corporate incentives to initiate internal investigations conducted by counsel.[126]

But while *Diversified Industries* is still good law, the concept of selective waiver is disfavoured by most federal circuit courts,[127] which routinely hold that selective disclosure of a document to the government constitutes complete waiver of the privilege. As the DC Circuit reasoned, the privilege was not designed to allow a client 'to pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality to obstruct others'.[128]

The Second Circuit confronted the issue of selective waiver in *In re Steinhardt Partners LP*.[129] While expressing reluctance to embrace selective waiver, the *Steinhardt* decision refused to foreclose the possibility that selective waiver may be found in some cases, at least where the disclosing party and the government share a common interest or the disclosing party has entered into an explicit agreement with the government to maintain the confidentiality of the disclosed materials.[130] As a result, in the Second Circuit, a case-by-case analysis of the facts is necessary to determine whether selective waiver may apply.[131]

The case of *SEC v. Herrera*[132] illustrates the risks of selective waiver inherent in making a proffer to the government. In *Herrera*, outside counsel conducted an internal investigation into certain apparent accounting errors in the company's books and records. During a subsequent SEC investigation, counsel was forthcoming to the SEC about documents that it uncovered over the course of its investigation, provided the SEC with a PowerPoint presentation that set forth its investigative steps and factual findings, and provided 'oral downloads' to the SEC of each of the 12 witness interviews it conducted. When former officers of the company were later sued in an SEC action, the defendants subpoenaed

122 572 F.2d 596 (8th Cir. 1977) (*en banc*).

123 Id. at 607.

124 Id. at 600.

125 Id. at 611.

126 Id.

127 See, e.g., *In re Pac. Pictures Corp.*, 679 F.3d 1121 (9th Cir. 2012) (asserting that the doctrine has been 'rejected by every other circuit to consider the issue since' *Diversified Industries*).

128 *Permian Corp.*, 665 F.2d at 1219–20.

129 9 F.3d 230 (2d Cir. 1993).

130 Id. at 236.

131 Id.

132 324 F.R.D. 258 (S.D. Fl. 2017).

© Law Business Research 2021

the records from the internal investigation during discovery, requesting (among other things) the law firm's written notes and memoranda from the witness interviews that had been described to the SEC and referenced in the PowerPoint presentation. The court rejected the law firm's argument that work-product protection still applied to the interview memoranda, finding that counsel's oral disclosures of their contents was the 'functional equivalent' of giving the SEC the memoranda themselves, removing any protection from them. The court acknowledged that the outcome may have been different had the external law firm only provided 'vague references' to the contents of the memo, or 'conclusions or general impressions' that were free of detail.[133] The court, reflecting the fact-specific nature of these determinations, however, did not find a broader subject matter waiver to the other findings referenced in counsel's presentation.

In *In re Grand Jury Investigation*,[134] in the context of the United States Special Counsel's Office (SCO) investigation of foreign interference in the 2016 presidential election, the SCO uncovered evidence that Paul Manafort (President Donald Trump's former campaign manager), his lobbying company and its employees made false statements in two letters submitted to the Foreign Agent Registration Act Registration Unit. In the first letter, counsel made factual representations that her clients did not have any agreements to provide services to a foreign entity. In the follow-up letter, counsel represented that one client could 'recall interacting' with consultants for a foreign entity, but did not recall meeting with or conducting outreach or facilitating any phone calls. The grand jury subsequently subpoenaed the attorney to testify about the communications underlying the factual representations in the letters. The attorney refused to answer the questions, citing the attorney–client privilege and work-product protection. The court found that counsel had waived, through voluntary disclosure, all the attorney–client privilege as to the contents of the letters, which 'made specific factual representations' that are 'unlikely to have originated from sources other than the Targets, and, in large part, were attributed to the Targets' recollections',[135] and extended the waiver to all communications on that same subject matter. The court also found that the crime-fraud exception provided an independent basis for waiver of privilege with respect to several of the questions posed to counsel in the grand jury.[136]

Some courts have suggested that production pursuant to a valid confidentiality agreement entered into with the government prior to the disclosure of

133 Id. at 264; see also *In re Fluor Intercontinental, Inc.*, 803 Fed. Appx. 697, 701-702 (4th Cir. 2 Mar. 2020) (rejecting an employee's attempt to compel production of his employer's investigation file following the disclosure of investigative findings to the Office of the Inspector General, finding that waiver cannot be inferred 'merely because the party's disclosure covers "the same topic" as that one which it had sought legal advice,' but only when 'there has been disclosure of protected communications')

134 No. 17-2336, 2017 WL 4898143 (D. D.C., 2 Oct. 2017).

135 Id. at *11.

136 Id. at *15.

© Law Business Research 2021

attorney–client privileged or work-product information effectively preserves the privilege and does not amount to a waiver as to third parties.[137] Consequently, if the company intends to disclose privileged material to the government, it should first attempt to obtain such an agreement from the government that it will keep the information confidential (a McKesson letter).[138] But even though future plaintiffs would not be parties to such an agreement, some courts have still found that the production of privileged materials pursuant to confidentiality agreements with the government nonetheless constitutes a waiver.[139] In light of federal courts' reluctance to find selective waiver, when a company voluntarily discloses documents or communications to government agencies, it must do so with the understanding that the documents and communications may lose the protection of the privilege and be subject to discovery by other parties, including private litigants.[140]

Taint teams 37.6

When a practising attorney's communications or work-product is seized as part of a government investigation, the DOJ has traditionally used an independent team called a 'taint team' to conduct an initial review of the documents to ensure there is no violation of the attorney–client privilege.[141] Taint teams are staffed with federal prosecutors and agents who are not otherwise involved with the underlying investigation.[142] The team's role is to perform a preliminary review of the materials that have been seized to filter out attorney–client

137 See, e.g., *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1127 (7th Cir. 1997); *In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1375 (D.C. Cir. 1984); *In re Natural Gas Commodity Litig.*, No. 03 Civ. 6186 (VM) (AJP), 2005 U.S. Dist. Lexis 11950, at *39 (S.D.N.Y. 21 Jun. 2005).

138 See David N Powers and Sara E Kropf, 'Disclosure of Internal Investigation Reports: A Legislative Solution to the McKesson Letter Dilemma', 32 *Sec. Reg. L.J.* 340, 341 (2004).

139 See, e.g., *In re Columbia/HCA Healthcare Corp.*, 293 F.3d at 302–04; *Westinghouse Elec. Corp.*, 951 F.2d at 1424–27, 1431.

140 Banks, in particular, often face pressure to share privileged materials with the government, both in the context of enforcement actions aimed at suspected wrongdoing and during routine regulatory oversight. With respect to US bank regulatory supervision, as a statutory matter, sharing privileged materials with bank supervisors results in a waiver of privilege only with respect to those supervisors; it does not waive applicable privileges with respect to third parties. Under Section 1828(x) of the Regulations Governing Insured Depository Institutions, the submission of information to 'the Bureau of Consumer Financial Protection, any [f]ederal banking agency, [s]tate bank supervisor, or foreign banking authority for any purpose in the course of any supervisory or regulatory process' shall not be construed as waiving privilege 'as to any person or entity other than such agency, supervisor, or authority'. 12 U.S.C. § 1828(x). This approach provides one of the few examples of federal statutes that explicitly contemplate selective waiver of the attorney–client privilege. Section 1828(x)'s companion statute, 12 U.S.C. § 1785(j), applies the same rule to credit unions.

141 Justice Manual § 9-13.420, at § E (2018), https://www.justice.gov/jm/jm-9-13000-obtaining-evidence. Taint teams are also known as 'privilege' or 'filter' teams.

142 Id.

© Law Business Research 2021

privileged communications before the materials are reviewed by the investigating team.[143]

Courts have scrutinised the DOJ's use of taint teams, identifying the potential for leaks of confidential information and the inherent conflict created when the same government office responsible for the review of the privileged materials has an interest in prosecuting the subject.[144] In rejecting the use of a government taint team for a privilege review, the Fourth Circuit observed that:

> *prosecutors have a responsibility to not only see that justice is done, but to also ensure that justice appears to be done. . . . Federal agents and prosecutors rummaging through law firm materials that are protected by attorney–client privilege and the work-product doctrine is at odds with the appearance of justice.*[145]

When the independence or propriety of a taint team is challenged, some courts have removed the task of reviewing the potential attorney–client documents from the purview of the DOJ, assigning the process to be governed by an independent, court-appointed official, such as a magistrate judge or a special master.[146]

In the face of scrutiny, the Criminal Division of the DOJ created a Special Matters Unit within the Fraud Section to standardise the use of taint teams. Attorneys in this unit work full-time – rather than *ad hoc* – to 'conduct, supervise, and litigate legal privilege matters and filter reviews on behalf of the Fraud Section's three litigating units'.[147] The Special Matters Unit's aim is to establish a set of 'uniform practices for handling evidence collection and review that implicate claims of attorney–client or other privileges', addressing some of the concerns previously raised by the courts regarding the potential conflicts

143 Id.

144 See *In re Grand Jury Subpoenas*, 454 F.3d 511, 523 (6th Cir. 2006) ('Furthermore, taint teams present inevitable, and reasonably foreseeable, risks to privilege, for they have been implicated in the past in leaks of confidential information to prosecutors. That is to say, the government taint team may have an interest in preserving privilege, but it also possesses a conflicting interest in pursuing the investigation, and, human nature being what it is, occasionally some taint-team attorneys will make mistakes or violate their ethical obligations. It is thus logical to suppose that taint teams pose a serious risk to holders of privilege, and this supposition is substantiated by past experience').

145 *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 183 (4th Cir. 2019).

146 See Alan Feuer and Benjamin Weiser, Former Judge Chosen to Review Materials Seized From Michael Cohen, *The New York Times* (26 Apr. 2018), https://www.nytimes.com/2018/04/26/nyregion/michael-cohen-investigation-special-master.html (where the court appointed a special master to oversee the process of reviewing seized materials); see also *In re Search Warrant*, 942 F.3d at 181 ('we are satisfied that the magistrate judge (or an appointed special master) – rather than the Filter Team – must perform the privilege review of the seized materials')

147 https://www.justice.gov/legal-careers/job/trial-attorney-special-matters-unit.

© Law Business Research 2021

arising from traditional taint teams.[148] Even still, courts continue to recognise the 'reasonably foreseeable risks to privilege' posed by taint teams, and some courts still view such practices as a potentially improper delegation of judicial functions to the executive branch.[149]

Disclosure to third parties 37.7

Generally, the attorney–client privilege is waived if the holder of the privilege voluntarily discloses or consents to the disclosure of any significant part of the communication to a third party or stranger to the attorney–client relationship.[150] A third-party agent may have communications with an attorney that remain covered by the attorney–client privilege if the agent's role is limited to helping a lawyer give effective advice to the client.[151] Whether disclosure to external consultants will constitute a waiver will depend on the surrounding facts and circumstances, including the purpose for the disclosure and the involvement of counsel with that third party.[152]

United States v. Kovel is the seminal case concerning the bounds of attorney–client privilege with respect to third-party consultants.[153] In *Kovel*, a law firm employed an accountant who was held in criminal contempt for refusing to testify about his conversations with the law firm's client under a claim of privilege.[154] In considering whether the accountant had a basis to assert attorney–client privilege, the Second Circuit recognised that there are situations 'where the lawyer needs outside help', and found that when the accountant assists in the 'effective consultation between the client and the lawyer which the privilege is designed to permit', the privilege should protect the communications.[155] The *Kovel* court analogised the accountant's role to that

148 Id.

149 *In re Search Warrant*, 942 F.3d at 177 (citing *In re Grand Jury Subpoenas*, 454 at 523).

150 See *In re Grand Jury Proceedings*, No. M-11-189 (LAP), 2001 WL 1167497, at *7 (S.D.N.Y. 3 Oct. 2001).

151 See *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961).

152 See, e.g., *Fed. Trade Comm'n v. GlaxoSmithKline*, 294 F.3d 141, 148 (D.C. Cir. 2002) (finding 'no reason to distinguish between a person on the corporation's payroll and a consultant hired by the corporation if each acts for the corporation and possesses the information needed by attorneys in rendering legal advice'); *NXIVM Corp. v. O'Hara*, 241 F.R.D. 109, 131–32 (N.D.N.Y. 2007) (finding that when attorney acted solely as coordinator of media relations, communications between attorney and client were not protected). See, generally, Michele DeStefano Beardslee, 'The Corporate Attorney–Client Privilege: Third-Rate Doctrine for Third-Party Consultants', 62 *SMU L. Rev.* 727, 744–55 (2009) (outlining the doctrine of the attorney–client privilege when third parties are involved).

153 296 F.2d 918 (2d Cir. 1961).

154 Id. at 919.

155 Id. at 922. Note, however, that not all attorney communications with accountants are within the bounds of the attorney–client privilege. Indeed, in I*QL-Riggig, LLC v. Kingsbridge Technologies*, No. 19 CV 6155, 2021 U.S. Dist. LEXIS 58939 (N.D. Ill. 29 Mar. 2021), the court found that attorney communications with an accounting firm hired to prepare the client's tax

© Law Business Research 2021

of an interpreter, which is sometimes necessary for the attorney effectively to communicate with his or her client.[156] The *Kovel* doctrine has been recognised by many courts as protecting attorney–client privilege in circumstances where a third party has specialised knowledge or skills that assist the attorney in rendering legal advice.[157] To preserve attorney–client privilege in such circumstances, the consultant is typically appointed directly by counsel and works under counsel's supervision. The mere hiring of the consultant through counsel, however, will not automatically cloak the third-party communications in privilege, if the consultant is otherwise performing a business function.[158] Instead,

returns were not protected under the attorney–client privilege. Id. at *5. The court further held that because the underlying tax advice was not privileged, conversations among lawyers concerning the advice were similarly not protected, reasoning that 'without showing that the privilege applies, focusing on waiver amounts to putting the cart before the horse'. Id. at *8.

156 Id. at 921.

157 See, e.g., *United States v. Adlman*, 68 F.3d 1495, 1499 (2d Cir. 1995) ('[u]nder certain circumstances . . . the privilege for communication with attorneys can extend to shield communications to others when the purpose of the communication is to assist the attorney in rendering advice to the client'); *United States v. Ackert*, 169 F.3d 136, 139 ('the inclusion of a third party in attorney–client communications does not destroy the privilege if the purpose of the third party's participation is to improve the comprehension of the communications between attorney and client'); *Exp.-Imp. Bank of the U.S. v. Asia Pulp & Paper Co.*, 232 F.R.D. 103, 113 (S.D.N.Y. 2005) (recognising, under *Kovel*, that 'communications with a financial adviser are covered by the attorney–client privilege if the financial adviser's role is limited to helping a lawyer give effective advice by explaining financial concepts to the lawyer').

158 See *In re Premera Blue Cross Customer Data Security Breach Litigation*, 296 F. Supp. 3d 1230, 1244–46 (D. Or. 2017) (declining to extend the attorney–client privilege to a third party consulting firm hired in the context of a data breach, where (1) the firm began its work on the project before counsel was retained, and (2) while the firm later entered into an agreement with the law firm directly, the consulting firm's scope of work did not otherwise change); *Durling v. Papa John's International, Inc.*, No. 16 Civ. 3592 (CS) (JCM), 2018 U.S. Dist. LEXIS 11584, at *14 (S.D.N.Y. 24 Jan. 2018) (declining to extend the attorney–client privilege protection to a consultant hired to analyse how a pizza company should reimburse its delivery drivers, finding that the consultants' 'role was not as a translator or interpreter of client communications', and that the company retained the consultant 'not to improve the comprehension of the communications between attorney and client, but rather to obtain information that [the company] did not already have'; *In re Restasis Antitrust Litigation*, 352 F. Supp. 3d. 207, 214–15 (E.D.N.Y. 2019) (rejecting the argument that outside consultants were 'functionally equivalent" of employees for the purposes of attorney–client privilege where (1) they did not exercise independent thinking on the company's behalf, (2) their advice supplemented the knowledge of other employees, (3) they did not appear as company representatives to third parties, (4) they did not spend a substantial amount of time working in the company's office, and (5) they did not seek legal advice from corporate counsel regarding their work at the company.).

© Law Business Research 2021

the company must show that the consultant's involvement was indispensable to – or served some specialised purpose in facilitating – the legal advice.[159]

For example, a client's statements to a private investigator hired by the client's attorney are often protected by the attorney–client privilege when the investigator acts as an agent of the attorney.[160] Similarly privileged (as work-product) are an investigator's interviews to gather background information for the attorney.[161] If, however, the investigator is going to be a fact witness concerning the information he or she has gathered, then all aspects of the investigator's fact gathering may be open to discovery, including statements by third parties to the investigator and the underlying factual data gathered by the investigator. Therefore, any work-product privilege that might have protected that information is waived by virtue of the private investigator's decision to testify.[162]

Courts have also extended attorney–client privilege to include public relations consultants under certain circumstances.[163] In particular, communications with public relations consultants have been found to maintain privilege if the primary purpose of the communication was to aid in the rendering of legal advice.[164] Such communications are found within the bounds of attorney–client privilege if the consultant provides services necessary to promote the attorney's effectiveness in the client's legal representation or the consultant is essentially an extension of the attorney under agency principles, or both.[165]

See Chapter 39 on publicity

159 See, e.g., *Narayanan v. Southern Global Holdings Inc.*, 285 F. Supp. 3d 604, 611–12 (W.D.N.Y. 2018).

160 See *U.S. Dept. of Educ. v. National Collegiate Athletic Ass'n.*, 481 F.3d 936, 937 (7th Cir. 2007) (recognising that, while there is no 'private investigators privilege,' there are circumstances where attorney–client privilege can 'embrace a lawyer's agents (including an investigator)'); see also, e.g., *Clark v. City of Munster*, 115 F.R.D. 609, 613 (N.D. Ind. 1987) (finding that statements made by a defendant to a private investigator employed by his attorney are protected by attorney–client privilege).

161 *Clark*, 115 F.R.D. at 614.

162 See *Brown v. Trigg*, 791 F.2d 598, 601 (7th Cir. 1986); *United States v. Nobles*, 422 U.S. 225 (1975) (finding that by electing to present the investigator as witness, the defendant waived his privilege as to information collected by the investigator and his attorney).

163 See *Grand Jury Subpoenas*, 265 F. Supp. 2d 321, 321 (S.D.N.Y. 2003); *Calvin Klein Trademark Trust v. Wachner*, 198 F.R.D. 53, 55 (S.D.N.Y. 2000).

164 See, e.g., *Grand Jury Subpoenas*, 265 F. Supp. 2d at 325; but see *Guiffre v. Maxwell*, No. 15 Civ. 7433 (RWS), 2016 U.S. Dist. LEXIS 58204, at *23–25 (S.D.N.Y. 2 May 2016) (finding that the media agent's involvement in otherwise privileged communications between the defendant and her lawyer destroyed any privilege protection because the defendant failed to establish (1) 'that [the agent] was necessary to implementing [the lawyer's] legal advice', (2) that she 'was incapable of understanding counsel's advice . . . without the intervention of a "media agent"' or (3) 'that [the agent] was translating information between [the lawyer] and Defendant in the literal or figurative sense')

165 See *Haugh v. Schroder Inv. Mgmt. N. Am., Inc.*, No. 02 Civ. 7955 (DLC), 2003 U.S. Dist. Lexis 14586, at *8 (S.D.N.Y. 25 Aug. 2003); *GlaxoSmithKline*, 294 F.3d at 148.

© Law Business Research 2021

Even with this guidance, the extent to which public relations consultants come within the bounds of attorney–client privilege is often unclear. For example, in *Calvin Klein Trademark Trust v. Wachner*, a court in the Southern District of New York refused to extend the attorney–client privilege to protect documents and testimony sought from Robinson Lerer & Montgomery (RLM), a public-relations firm retained by counsel to Calvin Klein.[166] In so ruling, the court held, *inter alia*, that the 'possibility' that communications between counsel and RLM might help counsel formulate legal advice was 'not in itself sufficient to implicate the privilege',[167] and that extending the privilege to the documents and communications at issue would apply the privilege too broadly because RLM did not appear to perform functions 'materially different from those that any ordinary public relations firm would have performed'.[168]

A few months later, in *In re Copper Market Antitrust Litigation*, a different judge from the same district court reached the exact opposite conclusion regarding the same public relations firm, finding that RLM acted as the company's 'spokesperson' when dealing with issues related to a copper trading scandal, and frequently conferred with counsel.[169] Under these facts, the court found that RLM acted as the 'functional equivalent of an in-house public-relations department with respect to Western media relations' and therefore found that the communications between RLM, the company and counsel were made for the purpose of facilitating the provision of legal advice.[170]

Similarly, in *FTC v. GlaxoSmithKline*, the US Court of Appeals for the DC Circuit found that communications with a public relations firm were protected by the privilege.[171] In so ruling, the court adopted the *Copper Market* court's rationale, crediting a party affirmation that the consultant became an 'integral member of the team assigned to deal with the issues [that] . . . were completely intertwined with [the client's] litigation and legal strategies'.[172] Hence, to improve the likelihood that communications with a public relations firm will be cloaked in attorney–client privilege, the firm should interact regularly with counsel, and act as an agent at counsel's direction.[173]

There are a growing number of federal courts declining to extend attorney–client privilege or work-product protection to forensic reports and related

166 198 F.R.D. at 54.

167 Id.

168 Id. at 55.

169 200 F.R.D. 213, 215 (S.D.N.Y. 2001).

170 Id. at 216.

171 294 F.3d 141 (2002).

172 Id.

173 But see *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1242 (D. Or. 2017). (Declining to extend the attorney–client privilege to communications with a public relations firm because 'drafting press releases relating to a security breach is a business function' and '[h]aving outside counsel hire a public relations firm is insufficient to cloak that business function with the attorney–client privilege')

© Law Business Research 2021

communications following data security breaches. For example, in *Rutter's*,[174] in response to notifications about potentially suspicious transaction activity, Rutter (a point of sale payments provider) hired outside counsel regarding its potential notification obligations and also a third-party security firm 'to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident'. When plaintiffs in litigation later sought production of the security firm's written report and related communications, the court determined that the work-product privilege did not apply because, among other things, litigation was not explicitly contemplated at the time the security firm was retained; and the record did not indicate that the report was reviewed by outside counsel before going to the client once the analysis was complete. The court found that the attorney–client privilege similarly did not apply because the security firm's statement of work focused on data collection, as to whether IT equipment had been compromised, and the related communications were factual in nature or otherwise did not implicate legal advice. The court found that the report and the related communications therefore did not have the primary purpose of providing or obtaining legal assistance, and were therefore not protected from disclosure.[175]

In sum, a party claiming the benefit of attorney–client privilege has the burden of establishing all of the essential elements to qualify for the protections of the privilege.[176] An attorney who wishes to consult with a non-attorney professional must seek to establish that the third party's involvement will facilitate legal advice from the beginning of the engagement.[177]

To support its claim that communications with, and documents generated by, a third party consultant are protected under the attorney–client relationship, counsel should memorialise the nature of the consultant's engagement in a *Kovel* letter. Such a letter should (1) state that counsel is retaining the consultant to assist with the provision of legal advice to the client, (2) instruct the consultant about specific tasks to be performed in support of the provision of that legal advice, (3) state that all work-product generated under the scope of the engagement is the property of counsel and (4) instruct the consultant to maintain the confidentiality of all information received or created in the course of the engagement. Further, the consultant should be guided in his or her actions by the attorney, rather than independently by the client.

---

174 *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220 (E.D. Pa. 22 Jul. 2021)

175 See also *Wengui v. Clark Hill*, No. 19-3195, 2021 U.S. Dist. LEXIS 5395, at *13–14 (D.D.C. 12 Jan. 2021).

176 See *Adlman*, 68 F.3d at 1500 (finding that a party claiming protection under the attorney–client privilege has the burden of proving each of the elements of such a privilege by contemporaneous proof of a *Kovel* agreement).

177 See, e.g., *In re G-I Holdings, Inc.*, 218 F.R.D. 428, 436 (D.N.J. 2003).

© Law Business Research 2021

37.7.1 Disclosure to the company's auditors

The disclosure of attorney–client privileged information to a company's external auditors ordinarily constitutes a subject-matter privilege waiver.[178] To the extent that counsel anticipates that the company's external auditors may require information about the status of an ongoing investigation, counsel should be prepared to communicate with auditors in a way that will limit any waiver of privilege. For example, counsel may provide the external auditor detailed information about the investigative process – including the structure, the personnel involved, the document preservation steps that were taken, general information about the process of reviewing documents and conducting interviews, and external consultants employed to assist in the investigation – which may provide the external auditors with a level of comfort about the comprehensive nature of the investigative process, without waiving the privilege regarding the substance of the investigation.

And while the disclosure of privileged information to auditors will likely waive the attorney–client privilege, work-product protection may remain intact if the auditor's interests are found not to be 'adverse' to the client. For instance, in *Merrill Lynch & Co v. Allegheny Energy Inc*,[179] Allegheny sought to compel discovery of two internal investigation reports (prepared by counsel) that Merrill Lynch had disclosed to its auditor, arguing that the disclosure constituted a waiver of any applicable privilege.[180] The court disagreed, stating that the 'critical inquiry' is whether the auditors 'should be conceived of as an adversary or a conduit to a potential adversary'.[181] The court held that 'any tension between an auditor and a corporation that arises from an auditor's need to scrutinize and investigate a corporation's records and book-keeping practices simply is not the equivalent of an adversarial relationship contemplated by the work-product doctrine'.[182] Consistent with the *Allegheny* court's guidance, if the client cannot avoid disclosure of privileged information to its auditors, counsel may be able to argue in subsequent civil litigation that work-product protection remains intact under this principle.

37.7.2 Disclosure to foreign governments

When analysing issues of waiver surrounding productions to foreign governments, courts of the United States tend to focus on whether the production of privileged material was compelled or voluntary. Where the submission is

178 See, e.g., *Chevron Corp. v. Pennzoil Co.*, 974 F.2d 1156, 1162 (9th Cir. 1992).

179 229 F.R.D. 441 (S.D.N.Y. 2004).

180 Id. at 444.

181 Id. at 447.

182 Id. at 448.

© Law Business Research 2021

compelled or where there was no opportunity to assert the privilege, United States courts will generally find that the privilege was not waived.[183]

Expert witnesses 37.8

Where government investigations involve complex financial transactions and other areas requiring specialised knowledge, counsel will often retain experts during the investigative stage to assist in their assessment of potential liability and in the building of the defence case. As with any external consultants, counsel should take steps to clarify that experts are being retained to assist counsel in their provision of legal advice, to maintain privilege over communications with the expert and their underlying analysis.

In the context of a criminal action that may follow an internal investigation, unless counsel determines that it would be advantageous to present expert analysis in conjunction with a report of its investigative findings to the government or regulatory authority, consulting expert materials will otherwise remain shielded from discovery as attorney–client privileged materials. If the defence intends to call an expert witness at trial, however, counsel may be obliged – at the government's request – to provide a written summary of the testimony that the defendant intends to offer at trial.[184] And while Federal Rule of Criminal Procedure 16 contemplates that the expert's underlying memoranda and other documents created during the case investigation will remain protected from disclosure,[185] counsel will still be required to produce documents that may qualify as 'statements' of a testifying expert under Federal Rule 26.2 prior to trial.[186]

In the context of civil litigation that may follow an internal investigation, however, expert discovery will be governed by Federal Rule of Civil Procedure 26. Prior to 2010, there was a significant risk that any documents

183 See *In re Grand Jury Proceedings*, 219 F.3d at 191 ('voluntary (as opposed to compelled) disclosure of documents to the SEC waived the company's work-product privilege as to other parties'); *Westinghouse Elec. Corp.*, 951 F.2d at 1427 n. 14 (finding privilege waiver in subsequent litigation where the party withdrew objections to SEC subpoena production and produced documents and noting that 'had [party] continued to object to the subpoena and produced the documents only after being ordered to do so, we would not consider its disclosure of those documents to be voluntary'); *In re Vitamin Antitrust Litig.*, No. MC 99-197 (TFH), 2002 WL 35021999, at *28 (D.D.C. 23 Jan. 2002) ('compulsion avoiding waiver requires that a disclosure be made in response to a court order or subpoena or the demand of a governmental authority backed by sanctions for noncompliance, and that any available privilege or protection must be asserted').

184 See Fed. R. Crim. P. 16(b)(1)(C).

185 See Fed. R. Crim. P. 16(b)(2)(A).

186 See Fed. R. Crim P. 26.2(f) (listing 'statement[s]' of testifying witnesses to include (1) a written statement that the witness makes and signs, or otherwise adopts or approves, (2) a substantially verbatim, contemporaneously recorded recital of the witness's oral statement that is contained in any recording or any transcription of a recording, or (3) the witness's statement to a grand jury, however taken or recorded, or a transcription of such a statement).

© Law Business Research 2021

provided to a testifying expert witness would be discoverable under Federal Rule 26, even if they were previously considered attorney–client privileged.[187] But the 2010 amendments to the rule made significant changes that strictly limited the discovery of communications between counsel and experts, including the discovery of draft expert reports. For example, Federal Rule 26(b)(4)(B) was added to provide work-product protection for drafts of expert reports or disclosure.[188] In addition, Federal Rule 26(b)(4)(C) was added to provide work-product protection for attorney-expert communications.[189] These amendments to Rule 26 were designed to protect counsel's work-product and ensure that lawyers may interact with experts 'without fear of exposing those communications to searching discovery'.[190]

Although the 2010 amendments provide significant protection for expert drafts and attorney–expert communications, counsel should still make efforts to limit the scope of potential disclosure by effectively managing a testifying expert's access to information and the development of the expert's opinions. For example, Federal Rule 26 does not preclude discovery of facts or data provided to the expert by an attorney, such as fact work-product prepared for the expert by counsel.[191] Consequently, counsel should create an inventory of all factual materials provided to a testifying expert and ensure that all such factual materials are accurate and final, and that such materials have been produced or are otherwise matters of public record. Further, where the committee notes accompanying Federal Rule 26 extend to 'any materials considered by' an expert, counsel should ensure that all of the facts made available to a testifying expert are based upon the record in the case, rather than as the result of attorney–client privileged communications.

Finally, while the amendment to Federal Rule 26 protects drafts of expert reports from disclosure, state court rules of civil procedure may vary as to whether such drafts are discoverable. If there is any question as to whether drafts of an expert report may be discoverable, especially if the matter is pending in a jurisdiction governed by state law, it may be advisable to negotiate a stipulation that explicitly extends the protection of the Federal Rules to expert discovery.

187 See *Synthes Spine v. Walden*, 232 F.R.D. 460, 463 (E.D. Pa. 2005) (collecting cases and requiring disclosure of privileged material); see also *Galvin v. Pepe*, No. 09-cv-104-PB, 2010 WL 3092640, at *6–7 (D.N.H. 5 Aug. 2010) (citing id.).

188 Fed. R. Civ. P. 26(b)(4) advisory committee's note.

189 Id.

190 See *Commodity Futures Trading Comm'n v. Newell*, 301 F.R.D. 348, 352 (N.D. Ill. 2014) (explaining that the government is not allowed to discover drafts of expert reports or attorney expert communications, unless communications fall within one of the three specific exceptions in Rule 26(b)(4)(C)).

191 Fed. R. Civ. P. 26(b)(4)(D).

© Law Business Research 2021

38

Publicity: The UK Perspective

Kevin Roberts, Duncan Grieve and Charlotte Glaser[1]

Introduction 38.1

Publicity is a necessary commercial consideration for any organisation, particularly within the context of a criminal or regulatory investigation, or a prosecution. Placing it high on the company's agenda ensures that organisations are able to respond swiftly and effectively to the announcement of such action, enabling them to steer some of the narrative promulgated by mainstream and social media. Any communications strategy needs to be carefully pitched and aligned with legal advice to avoid unintended adverse consequences. Mistakes in communications can have a real impact on prosecutorial behaviour and a company's ability to effectively engage with prosecution agencies.

This chapter sets out a number of factors an organisation should consider before and after the commencement of an investigation or prosecution. It goes on to consider the legislation that governs the publication of information and the effect that remote hearings may have on the principle of open justice.

Before the commencement of an investigation or prosecution 38.2

Identify a public relations team 38.2.1

One of the first things an organisation should think about when considering publicity in an investigation or prosecution is who should be at the table when news breaks. Alongside the most obvious candidates (chief executive officer, head of public relations), individuals such as the chief technology officer and the chief data officer or data protection officer should also be considered. That is because once an organisation is placed under investigation or made subject

1 Kevin Roberts is a partner, and Duncan Grieve and Charlotte Glaser are associates, at Cadwalader, Wickersham & Taft LLP.

© Law Business Research 2021

to a prosecution, it will have to put in place document holds to ensure that information is not inadvertently destroyed. Equally, data that is required to be handed over to enforcement agencies is likely to contain personal data, as defined by Regulation EU 2016/679 (General Data Protection Regulation (GDPR)). Therefore, data processors should contemplate how such data will be processed in compliance with the GDPR.

Beyond internal stakeholders, an organisation should consider whether to engage reputable and experienced public relations advisers who can help to coordinate any engagement that the company has with other external stakeholders and mainstream media. In addition, if it has not already done so, the company should think about whom it intends to instruct as external counsel.

38.2.2 Determine the remit of the public relations team and a response plan

Once an organisation has identified who will be part of the core public relations team, it will need to devise a response plan; that is, determine what needs to be done upon becoming aware of the investigation or prosecution. Actions relating to the response plan can be split into two categories: internal and external. The public relations team will need to determine the role of each member – including who has ultimate sign-off on each decision – and to assign each (internal and external) action to one or more individuals. The team needs to be able to act nimbly and to make and effect decisions in real-time. Many organisations have difficulty in delegating appropriately and getting ahead of the narrative. An ineffective and purely reactive team will lead to poor internal and external relations.

38.2.3 Undertake tabletop exercises

Individuals often do not operate at peak performance when they are panicked or caught off-guard. The same can be said of organisations. It can be worthwhile for a company to invest time in carrying out a rehearsal. A simulation can help to highlight common pitfalls, such as a senior executive providing comments to the press that are not founded in fact. It can also ensure that an organisation can respond to an announcement promptly and effectively, so as to mitigate any damage that can flow from it. Appropriate media training for any individuals interacting with the press is essential.

38.2.4 Self-reporting

If an organisation decides to self-report to a prosecutor, where there has previously been no publicity on the relevant conduct, that will afford the company more time to consider how to respond to media interest once the self-report has been made public. It also places a company in the advantageous position of knowing in more detail the facts surrounding the relevant conduct, minimising its risk of having to provide subsequent corrections or clarifications. After self-reporting, a company would be well advised to agree any media reporting with prosecutors.

© Law Business Research 2021

Following the commencement of an investigation or prosecution 38.3

Internal actions and communications 38.3.1

Following the commencement of an investigation or prosecution, the public relations team will need to promptly convene a briefing meeting, after which the team will need to begin implementing the response plan. As mentioned above, the response plan can be divided into internal and external actions. External actions are considered below. Internal actions will probably include:

- determining whether document holds should be placed over any information;
- ensuring that the processing of any personal data complies with the GDPR;
- determining whether to conduct a parallel internal investigation and employee interviews;
- considering whether it is likely that a search warrant will be executed and making preparations; and
- if the company is publicly listed, determining what disclosures need be made as a result of the company's public listing.

An organisation will also need to consider when and how to communicate with its internal stakeholders. To do that, it will first need to identify the internal stakeholders. These will include employees, the board of directors and shareholders.

When to communicate with internal stakeholders? 38.3.1.1

When information about the investigation or prosecution is made public, internal stakeholders are likely to become aware of it very quickly. As a result, they should be communicated with promptly. The primary intention of communication should be to provide information and reassurance. It should additionally ask employees not to comment individually and address what they should do if they are approached by the media.

How to communicate with internal stakeholders? 38.3.1.2

An organisation will want to ensure that a consistent message filters down through the organisation. These types of communications can be most effective when they come from one source, typically the chief executive officer, and address all internal stakeholders at the same time.

External actions and communications 38.3.2

In any investigation or prosecution, it will be necessary to liaise with prosecutors. Those communications will often not be conducted in public and will be led by the company's general counsel or head of legal. Where possible, companies should avoid commenting upon a case through general counsel as that can cause unnecessary complications with external agencies at a later stage.

In addition, an organisation will need to consider whether to issue a press release and the media platform, or platforms, on which to do so. In light of the expanding number of outlets through which organisations can communicate

© Law Business Research 2021

with stakeholders and the wider public, it is no longer necessary for a company to solely engage with, if at all, mainstream media. A company may consider that there is no need to engage in any oral broadcast and instead communicate via platforms such as Twitter and Facebook. Alternatively, or additionally and as is common, an organisation may issue a press release on its website.

If an organisation does wish to make a public oral statement, a great deal of planning should go into determining how, when and where the statement will be made and what can be done to mitigate the risks. Those risks were all too evident from the fallout of Prince Andrew's interview with the BBC about his relationship with Jeffrey Epstein, a convicted sex offender. Indeed, once an organisation has agreed to provide an interview or to accept questions from the media, although what can be discussed may have been agreed in advance, few questions will in reality be off limits, and a failure to answer a particularly difficult question could be seen unfavourably. Companies must also be careful not to prejudice an active investigation or prosecution, or make comments that are not founded in fact, which could force a damaging retraction or correction. The importance of ensuring that all public statements and comments are consistent and accurate may mean that, particularly at the early stages of an investigation or prosecution, it is necessary to keep all statements short and based on information within a company's knowledge.

However, as much as an organisation may wish to escape direct communication with the mainstream media, it is unlikely that it will be able to insulate senior executives, who regularly appear in public, from being asked questions. As a result, consideration should be given to how those individuals should be expected to respond. Preparation and training for senior executives is essential. A senior executive appearing at annual meetings or a conference must be well briefed and prepared to answer difficult questions from journalists.

After an organisation has decided to make a public statement, and determined its form, the company will have to decide when to communicate it. Depending on the facts, organisations may choose to be proactive, having considered that this approach allows them to influence the narrative and maintain public confidence. Following a public statement, ongoing monitoring and correction of media content pertaining to the investigation or prosecution will need to be maintained. That role may be assigned to a member of the public relations team.

38.4 Following the conclusion of an investigation or prosecution

38.4.1 Communications with relevant prosecuting authorities

Where an investigation has concluded without further action being taken against a company, or a prosecution of a company has led to an acquittal, the company should ensure that all media content relating to the investigation or prosecution reflects this.

© Law Business Research 2021

Debrief 38.4.2

Once an investigation or prosecution has concluded, regardless of the legal outcome, an organisation may find value in reflecting how the company conducted itself throughout the process, and consider lessons learned should it unfortunately find itself in a similar situation in the future.

Legislation governing the publication of information 38.5

Common law principle of open justice and derogations 38.5.1

Open justice 38.5.1.1

The constitutional principle of open justice prescribes that justice should be administered in a way that allows all to see it. The principle is enshrined in Article 6 (the right to a fair trial) of the European Convention on Human Rights (ECHR) and comprises one of the core tenets upon which the United Kingdom's legal system is founded. The Criminal Procedure Rules state that when courts are exercising their powers in relation to reporting, and furthering the overriding objective of dealing with cases justly, they must have regard to the importance of dealing with criminal cases in public, and allowing a public hearing to be reported to the public.[2] The principle is motivated by the desire (among others) to ensure that courts and tribunals can be held accountable for the decisions that they make, and to maintain public confidence in the way that those decisions are made.

In 2019,[3] Lady Hale, the former President of the United Kingdom Supreme Court, held that the common law principle applies to all courts and tribunals exercising 'the judicial power of the state'.[4] Those institutions enjoy an inherent jurisdiction to 'determine what that principle requires in terms of access to documents or other information placed before [them]'.[5] However, the principle is not absolute; there are certain circumstances, albeit limited and exceptional, in which courts and tribunals can exercise their inherent jurisdiction, or jurisdiction under the Human Rights Act 1998,[6] to derogate from it.[7]

Derogations from the principle of open justice 38.5.1.2

Any derogation from the principle of open justice must be necessary and based on clear and cogent evidence.[8] An organisation can appeal a Crown Court's decision to derogate from the principle.[9]

---

2 Criminal Procedure Rule 6.2(1).

3 *Cape Intermediate Holdings Ltd v. Dring* (for and on behalf of Asbestos Victims Support Groups Forum UK) [2019] UKSC 38.

4 ibid., at 36.

5 ibid., at 41.

6 Which transposes the ECHR into UK domestic law.

7 *Khuja v. Times Newspapers Limited & Ors* [2017] UKSC 49, at 14.

8 *Scott v. Scott* [1913] AC 417.

9 Criminal Justice Act 1988, s.159.

© Law Business Research 2021

Suspects in criminal investigations before they are charged

In 2020, the Court of Appeal (in England and Wales) reaffirmed that individuals under police investigation are entitled to a reasonable expectation of privacy before they are charged.[10] The Court held that there is 'little justification for a hierarchy of offences' to which the reasonable expectation applies.[11] In *ZXC v. Bloomberg*, the allegations concerned fraud, bribery and corruption. Nevertheless, there may be occasions where that reasonable expectation of privacy is 'significantly reduced, perhaps even to extinction, due to the public nature of the activity under consideration', such as in the cases of rioting and electoral fraud.[12]

The case followed an earlier decision by the High Court in a case where Sir Cliff Richard successfully sued the BBC for its coverage of a police raid on his home as part of an investigation into historical child sexual abuse allegations.[13] In that case, the Court held that 'as a matter of general principle, a suspect has a reasonable expectation of privacy in relation to a police investigation'.[14]

The Leveson Report on the culture, practices and ethics of the British media was published in 2012. In relation to the naming of suspects, it concluded that 'save in exceptional and clearly identified circumstances (for example, where there may be an immediate risk to the public), the names or identifying details of those who are arrested or suspected of a crime should not be released to the press or the public'.[15]

In 2017, the College of Policing published its 'Media relations' guidance (the Media Guidance). It states that 'suspects should not be identified to the media (by disclosing names or other identifying information) prior to the point of charge except where justified by clear circumstances, e.g. a threat to life, the prevention or detection of crime or a matter of public interest and confidence'.[16]

However, the existence of guidance and legal authority on the issue does not mean that either is always followed in practice. Suspects who have not yet been charged are routinely identified by the media, and in some cases, in public statements issued by prosecution agencies. Individuals about whom false statements are made in the media are able to sue those responsible in the civil courts for libel. Nevertheless, while such recourse exists in principle, the case brought by Johnny Depp against News Group Newspapers Ltd[17] illustrates that the further reputational damage caused by media coverage of a libel suit can outweigh any potential benefit.

10 *ZXC v. Bloomberg LP* [2020] EWCA 611.

11 ibid., at 84.

12 ibid., at 84.

13 *Sir Cliff Richard OBE v. The British Broadcasting Corporation & Anor* [2018] EWHC 1837 (Ch).

14 ibid., at 248.

15 Volume 2, Chapter 4, para. 33, page 984.

16 See para. 3.2.

17 *John Christopher Depp II v. News Group Newspaper Ltd* [2020] EWHC 2911 (QB).

© Law Business Research 2021

Suspects in criminal investigations after they are charged

Once a suspect has been charged, he or she is no longer able to claim a reasonable expectation to privacy.[18] In that regard, the Media Guidance states: 'Those charged [which includes those who receive a summons to court] with an offence should be named unless there is an exceptional and legitimate policing purpose for not doing so or reporting restrictions apply. This information can be given at the point of charge.' It also states that police forces should 'proactively' release information relating to charges in serious crimes, such as rape or murder.[19]

In the event that charges are withdrawn before a person first appears in court, the Media Guidance advises that such information should be proactively released 'as soon as possible'.[20]

Persons named in open court proceedings

Persons who are named in open court are not entitled to a reasonable expectation of privacy.[21] That includes suspects who have not been charged, and who would therefore ordinarily be entitled to an expectation of privacy, but have already been named in open court as a result of being referred to in charges laid against others. However, if it is known that a person not directly involved in criminal proceedings intends to be referred to in open court before in fact they are, an application for anonymity can be made to the court.[22]

Businesses

In relation to businesses, the Media Guidance states that:

> *Businesses may be routinely identified as part of police investigations, for example as part of an appeal for witnesses. In some cases operational policing reasons may prevent businesses being identified, for example where it could impact upon an investigation. The need to protect private information may also prevent businesses being identified, e.g. in circumstances where identifying a business might indirectly identify a suspect. Decisions should be taken on a case by case basis.*[23]

Publicity restrictions where absolute ECHR rights are engaged

A number of rights afforded to individuals under the ECHR are absolute and therefore no derogation is permitted. These include the right to life (Article 2) and the right to freedom from torture or inhumane or degrading treatment or punishment (Article 3). As a result, where those rights are engaged, a court or

18 *ZXC v. Bloomberg LP* [2020] EWCA 611.

19 See para. 4.5.

20 id.

21 *Khuja v. Times Newspapers Limited & Ors* [2017] UKSC 49.

22 id.

23 See para. 4.7.

© Law Business Research 2021

tribunal may have to suspend the application of open justice in some way. Such circumstances may be found in international cases where individuals relevant to the proceedings are based in other jurisdictions.

Publicity restrictions where qualified ECHR rights are engaged

In circumstances where qualified rights under the ECHR are engaged, such as the right to respect for private and family life (Article 8), the right to a public hearing (Article 6) and the right to freedom of expression and information (Article 10), a court or tribunal must undertake a balancing exercise to determine whether a person's privacy rights should weigh in favour of a proportionate interference with Article 10.[24]

38.5.2 Statutory reporting restrictions in the criminal courts

38.5.2.1 Reporting restrictions generally

Courts and tribunals have no inherent jurisdiction or power derived from common law to impose reporting restrictions.[25]

38.5.2.2 Automatic reporting restrictions

The strict liability rule

Pursuant to sections 1 and 2 of the Contempt of Court Act 1981, if published information (including written and oral publications), or other communications in whatever form, create a substantial risk that the course of justice in active proceedings will be seriously impeded or prejudiced, that conduct will amount to the offence of contempt of court. As it is a strict liability offence, it does not matter whether the relevant person intended to interfere with the course of justice. However, a person will not be guilty of the offence if he or she contemporaneously, and in good faith, published a fair and accurate report of the public legal proceedings.[26]

In relation to such proceedings, in circumstances where the court considers it necessary to avoid a substantial risk of prejudice to the administration of justice, it may order that the publication of any report of the proceedings be postponed for a period that it deems necessary.[27]

Pre-trial hearings, preparatory hearings and dismissal hearings

Automatic reporting restrictions exist in relation to the following:

- pretrial hearings;[28]

24 *Re Guardian News and Media Ltd & Ors in HM Treasury v. Ahmed & Ors* [2010] UKSC 1.

25 *Khuja v. Times Newspapers Limited & Ors* [2017] UKSC 49, at 18.

26 Contempt of Court Act 1981, s.4(1).

27 ibid., s.4(2).

28 Criminal Procedure and Investigations Act 1996, s.41; Magistrates' Court Act 1980, s.8A.

© Law Business Research 2021

- preparatory hearings that are held in relation to, among other cases, serious fraud cases. However, the name of the defendant and the offence with which they have been charged may be reported; and [29]
- dismissal applications in the Crown Court relating to persons sent for trial there under sections 51 and 51A of the Crime and Disorder Act 1998. As with preparatory hearings, the name of the defendant and the offence with which they have been charged can be reported.[30]

The restrictions set out above cease to apply once the trial has concluded. Although, a court may remove or limit the restrictions before that time in certain circumstances. In relation to pretrial and preparatory hearings, if the defendant objects to an order removing or limiting the restrictions, a court may only make the order after hearing representations from the defendant (which must not be reported), and, upon hearing those representations, being satisfied that it is in the interests of justice to make it.[31]

Prosecution appeals

Automatic reporting restrictions apply in relation to prosecution appeals. However, a court may make an order to limit or not to apply the restrictions. If the defendant objects to the making of such an order, similarly to pretrial and preparatory hearings, the order can only be made if, after hearing the defendant's objections (which must not be reported), the court considers that it is in the interests of justice to make it.[32]

Discretionary reporting restrictions 38.5.2.3

Deferred prosecution agreements

A court may order that the publication of a deferred prosecution agreement is postponed for such period as the court deems necessary, if the court considers that postponement is necessary to avoid a substantial risk of prejudice to the administration of justice.[33] In such cases, a company will have agreed a statement of facts that will likely form the basis of any subsequent Serious Fraud Office press release.

29 Criminal Procedure and Investigations Act 1996, s.37; Criminal Justice Act 1987, s.11.

30 Crime and Disorder Act 1998, Schedule 3, para. 3.

31 Criminal Procedure and Investigations Act 1996, s.41; Criminal Procedure and Investigations Act 1996, s.37; Criminal Justice Act 1987, s.11.

32 Criminal Justice Act 2003, s.71.

33 Crime and Courts Act 2013, Schedule 17, para. 12. This power was exercised in relation to the deferred prosecution agreement (DPA) between Serco and the Serious Fraud Office (SFO). In that case the judge delayed publication of the statement of facts (which are often published with the DPA) in order that the SFO's investigation into potential criminal conduct committed by individuals was not prejudiced.

© Law Business Research 2021

38.5.3 Public access to information and documents from criminal courts

In circumstances where documents have been placed before a judge and referred to in open court, the court has an inherent jurisdiction to disclose them.[34] That is in part because the principle of open justice exists not only to ensure that court decisions are made lawfully and in the absence of any impropriety, but also 'to enable the public to understand and scrutinise the justice system of which the courts are the administrators'.[35]

Where a party makes an application for the disclosure of such documents, the following test, as set out by Lord Justice Toulson (as he then was), should be applied by the court:

> *The default position should be that access should be permitted on the open justice principle; and where access is sought for a proper journalistic purpose, the case for allowing it will be particularly strong. However, there may be countervailing reasons . . . I do not think that it is sensible or practical to look for a standard formula for determining how strong the grounds of opposition need to be in order to outweigh the merits of the application. The court has to carry out a proportionality exercise which will be fact-specific. Central to the court's evaluation will be the purpose of the open justice principle, the potential value of the material in advancing that purpose and, conversely, any risk of harm which access to the documents may cause to the legitimate interests of others.*[36]

38.5.4 GDPR and the Data Protection Act 2018

The UK Data Protection Act 2018 (DPA 2018) gives effect to the provisions contained in the GDPR. An organisation is likely to fall within the definition of a data processor, as defined in the legislation. As such, it must ensure that all personal data is processed in compliance with the GDPR. That could mean that the release of certain information into the public domain, whether via a press release, public statement or other such channel, is prohibited under data protection legislation. That obligation underlines the significance of ensuring that a company's data protection officer forms part of the public relations team and sits in on any related briefings.

38.5.5 Tension between publicity and privilege

Once an investigation or prosecution has commenced, a company may claim litigation privilege over certain documents that come into existence for the sole or dominant purpose of litigation. Equally, it will be able to claim privilege over certain documents relating to legal advice sought from or provided by the

34 *R (Guardian News and Media Limited) v. City of Westminster Magistrates' Court* [2012] EWCA Civ 420.

35 ibid., at 79.

36 ibid., at 85.

© Law Business Research 2021

company's lawyers. When communicating with stakeholders and mainstream media, a company must be careful to ensure that it does not inadvertently waive privilege. Unscripted statements from senior executives regarding an ongoing investigation may inadvertently waive privilege, which could have severe consequences. This is another reason why it is generally better for general counsel or members of the company's in-house legal team not to be involved in directly speaking with the media.

The changing landscape: remote hearings and open justice 38.6

Before 2020, remote hearings were reserved for the most straightforward and largely administrative hearings in the criminal courts, such as case management hearings. However, the onset of a global pandemic has exponentially advanced the UK court and tribunals system's ability and willingness to undertake remote hearings for all types of hearings.

On 25 March 2020, the Coronavirus Act 2020 came into force and increased the range of hearings that can be conducted by way of video or audio link by inserting amendments into a number of Acts that govern proceedings in the criminal courts; including, the Courts Act 2003, the Criminal Justice Act 2003 and the Crime and Disorder Act 1998. Among other things, the amendments allow for fully remote hearings.

The speed at which such change was implemented, to ensure that access to justice was not further delayed, was commendable. It was a novel approach to criminal hearings that raised the question of how the principle of open justice could be upheld when there no longer existed a dedicated space for members of the public and journalists to attend. The provisions set out in the Coronavirus Act went some way to addressing that question. Where a court directs that proceedings are to be conducted wholly as video proceedings, it is afforded the discretion to 'direct that the proceedings are to be broadcast (in the manner specified in the direction) for the purpose of enabling members of the public to see and hear the proceedings'.[37] A similar provision exists for audio proceedings.[38]

Remote proceedings of all kinds are now well established. As at 14 May 2021, approximately 225,000 hearings had taken place using the Cloud Video Platform[39] in magistrates' courts and Crown courts.[40] Owing to the need for all parties to expose themselves to and familiarise themselves with such technology in a relatively short period, on the whole, remote hearings appear to be working well. Contested hearings and hearings that involve vulnerable witnesses and defendants continue to present challenges.

37 Schedule 25, para. 85A(1).

38 Schedule 25, para. 85A(2).

39 The videoconferencing technology rolled out by HM Courts and Tribunals Service to support remote hearings across England and Wales.

40 https://www.gov.uk/guidance/hmcts-services-remote-hearing-channels-crime.

© Law Business Research 2021

39

Publicity: The US Perspective

Jodi Avergun[1]

39.1 Restrictions in a criminal investigation or trial

39.1.1 Generally

The US Constitution guarantees defendants in criminal cases the right to a speedy and public trial. It also guarantees all Americans freedom of speech and freedom of the press. In the trial setting, these constitutional rights are sometimes in conflict. For instance, although freedom of the press is guaranteed, media reports about a case can taint a pool of potential jurors or might allow sworn jurors to learn about matters not in evidence. Accordingly, lawyers practising in the United States must be aware of the multiple, conflicting rights that affect judicial proceedings. These rights include the public's right of access to trial proceedings,[2] the media's right to report what occurs in court,[3] the liti-

1 Jodi Avergun is a partner at Cadwalader, Wickersham & Taft LLP.

2 *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575–81 (1980) (holding that the right of the public and the press to attend criminal trials is guaranteed under the First and Fourteenth Amendments, and that, absent an overriding interest established after a factual hearing, the trial of a criminal case must be open to the public). In 1986, the US Supreme Court extended its ruling in *Richmond Newspapers* to jury selection. *Press-Enterprise Co. v. Superior Court of California*, 478 U.S. 1 (1986).

3 *Estes v. State of Tex.*, 381 U.S. 532, 541–42 (1965) ('Reporters of all media, including television, are always present if they wish to be and are plainly free to report whatever occurs in open court through their respective media.').

© Law Business Research 2021

gants' freedom of speech[4] and the defendant's right to a fair trial.[5] No one right is absolute, and each is limited by various rules and regulations.[6]

A lawyer's ethical obligations, for example, may limit the attorney's First Amendment right to speak publicly about a case. Under the American Bar Association Model Rules of Professional Conduct, which have been adopted, in whole or in part, by the vast majority of US jurisdictions, a lawyer who has or is participating in a matter must not make an 'extrajudicial statement' that 'will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter'.[7] In federal criminal cases, prosecutors must also comply with these rules, as well as those published in the Justice Manual, limiting the information a prosecutor may disclose or the issues he or she may comment on.[8]

Apart from the rules prohibiting a lawyer from publicly commenting on a pending case, a lawyer's professional duty to keep client matters confidential may also prevent him or her from publicising information about a case.[9]

Investigatory and pretrial stage 39.1.2

During the investigative stage of the case, before charges have been filed, a court cannot limit an individual involved in an investigation from making public statements about the case. But because such statements can be used by a prosecutor against a defendant in a subsequent criminal proceeding (either as substantive evidence or to demonstrate that the individual waived his or her right to remain silent), lawyers often counsel their clients to exercise their free speech rights carefully, if at all. Prosecutors are more constrained, however. The Justice Manual provides that a prosecutor cannot make public statements about a case if there is substantial likelihood that the statement will materially prejudice an adjudicative proceeding.[10] Similarly, prosecutors, but

4 *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1074-75 (1991) (describing the bounds to which limitations may be placed on a lawyer's First Amendment right to free speech).

5 *Press-Enter. Co. v. Superior Court of California, Riverside Cty.*, 464 U.S. 501, 508 (1984). ('No right ranks higher than the right of the accused to a fair trial.')

6 See *United States v. Gerena*, 869 F.2d 82, 85 (2d Cir. 1989). ('The district court must balance the public's right of access against the privacy and fair trial interests of defendants, witnesses and third parties.'); *United States v. Rajaratnam*, 708 F. Supp. 2d 371, 374 (S.D.N.Y. 2010) (explaining that courts 'must balance the right [to access criminal proceedings] against other important values, like the Sixth Amendment right of the accused to a fair trial').

7 Model Rules of Prof'l Conduct R. 3.6(a) (2019).

8 U.S. Dep't of Justice, Justice Manual, § 1-7.000 (Confidentiality and Media Contacts Policy), available at https://www.justice.gov/jm/jm-1-7000-media-relations.

9 See, e.g., *Sealed Party v. Sealed Party*, No. 04-2229, 2006 U.S. Dist. LEXIS 28392 (S.D. Tex. 4 May 2006) (finding breach of fiduciary duty where attorney published a press release disclosing the terms of a confidential settlement).

10 U.S. Dep't of Justice, Justice Manual, § 1-7.000 (Confidentiality and Media Contacts Policy), available at https://www.justice.gov/jm/jm-1-7000-media-relations.

© Law Business Research 2021

not individual witnesses, are prohibited from disclosing any matters that occur before a grand jury.[11]

Once charges have been filed, however, courts have greater ability to insulate their proceedings from the prejudicial effects of any publicity.[12] A judge's failure to exercise this power may, under certain circumstances, violate a defendant's right to a fair trial.[13] In widely publicised cases, the local rules may authorise the court to issue orders governing extrajudicial statements by parties, witnesses and attorneys, and the seating and conduct of spectators, as well as the sequestration of jurors and witnesses.[14] Sometimes, litigants can attempt to prevent the public disclosure of private or prejudicial information prior to trial by filing their documents under seal and pursuant to protective orders.[15] However, because the First Amendment guarantees the public's right of access to governmental proceedings, sealed filings can only be made with the court's permission and upon a showing of necessity or that unfair prejudice might result from public dissemination. Accordingly, motions to seal proceedings are not lightly granted, and government lawyers in particular are severely limited in their ability to file motions under seal or to consent to their opponent's request to close proceedings.[16] Rather than seal proceedings or files, courts must consider whether a change of venue, jury sequestration or gag orders, among other techniques, would adequately protect the rights of the parties.

---

11 Rule 6(e)(2) prohibits a grand juror, interpreter, court reporter, operator of a recording device, person who transcribes recorded testimony, attorney for the government, or person to whom a proper disclosure is made under Rule 6(e)(3)(a)(ii) or (iii) from disclosing a matter occurring before the grand jury. Fed. R. Crim. P. 6(e). The rule does not impose any obligation of secrecy on witnesses.

12 See, e.g., *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976) (holding that a court may enter a 'gag' order prohibiting the reporting of evidence adduced at an open preliminary hearing if it finds 'a clear and present danger that pre-trial publicity could impinge upon the defendant's right to a fair trial').

13 *Sheppard v. Maxwell*, 384 U.S. 333 (1966) (holding that failure of a state trial judge to protect the defendant in a murder prosecution 'from the inherently prejudicial publicity which saturated the community and to control disruptive influences in the courtroom' deprived the defendant of a fair trial consistent with the Due Process Clause of the Fourteenth Amendment).

14 See, e.g., L. Cr. R 57.7(c): S.D.N.Y. L. Cr. R 23.1(h).

15 *Johnson v. Greater Se. Cmty. Hosp. Corp.*, 951 F.2d 1268, 1277 (D.C. Cir. 1991) (noting that, in permitting a party to file a document under seal, should consider '(1) the need for public access to the documents at issue; (2) the extent to which the public had access to the documents prior to the sealing order; (3) the fact that a party has objected to disclosure and the identity of that party; (4) the strength of the property and privacy interests involved; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced'); see also *Strauss v. Credit Lyonnais, S.A.*, No. 06-CV-702, 2011 WL 4736359, at *4 (E.D.N.Y. 6 October 2011) (approving a protective order that governs the filing of documents under seal as well as the public filing of documents).

16 28 C.F.R. § 50.9.

© Law Business Research 2021

Courts sometimes issue gag orders to protect against undue pretrial publicity. For example, Judge Amy Berman Jackson, who presided over the criminal case against Paul Manafort (President Donald Trump's former campaign manager), issued a gag order in the trial, barring anyone involved in the case from making public statements that might taint it. In her written order, Judge Jackson stated that she wanted to make sure the trial was fair and that potential jurors were not influenced by pretrial publicity.[17] It is far more common, however, for courts to deny gag orders, even in cases where the public interest in the case is quite high. For example, despite the negative publicity and strong public reaction surrounding former Jeffrey Epstein associate Ghislaine Maxwell's sex-trafficking case, the court denied Maxwell's motion to prohibit 'the Government, its agents and counsel for witnesses from making extrajudicial statements' about the case, holding that the public comments cited to date had not impeded Maxwell's right to an impartial jury.[18] However, in July 2021, Judge Nathan ordered counsel associated with the case, whether or not they had filed a notice of appearance, to comply with Southern District of New York Local Criminal Rule 23.1, to refrain from making public statements that could interfere with a fair trial or otherwise prejudice the due administration of justice.[19]

In another case charging Trump confidant Steve Bannon, the court again stopped short of issuing a gag order, even in light of a defendant's comments on social media that the charges against him were a 'witch hunt' and that he and the other defendants were 'political prisoners'. Rather, the court cautioned both sides that inappropriate public comments would not be tolerated and that it expected that both sides would be able to abide by its ruling.[20]

Upon a showing that pretrial publicity about the case will prevent the empanelment of an impartial jury or will otherwise prejudice the defendant, the defendant can move to have the case transferred to another district.[21]

In the *Manafort* matter, defence attorneys were concerned that the extensive pretrial press coverage of all aspects of the investigation and indictment would taint the jury panel. Manafort moved for a change of venue, arguing that extensive media coverage of the investigation and subsequent indictment infected the jury pool in Alexandria, Virginia, where the indictment was brought. The court denied that motion, arguing that the media coverage surrounding the

17 *United States of America v. Manafort et al.*, No. 1:17-CR-00201-ABJ (D.D.C. filed 8 Nov. 2017), ECF No. 38.

18 *United States v. Maxwell*, 20-CR-00330, Order, ECF No. 28 (D) (S.D.N.Y., 23 Jul. 2020).

19 *U.S. v. Maxwell*, No. 1:20-CR-00330-AJN (S.D.N.Y. filed 30 Jul. 2021) ECF No. 315.

20 Pete Brush, Bannon Gets Trial Date For Alleged Wall Funding Fraud, *Law360* (31 Aug. 2020), https://www.law360.com/articles/1305916/bannon-gets-may-trial-date-for-alleged-wall-funding-fraud.

21 Fed. R. Crim. P. 21(a); see also *Sheppard*, 384 U.S. at 363 (requiring the defendant to show 'a reasonable likelihood that prejudicial news prior to trial will prevent a fair trial').

© Law Business Research 2021

case had not turned it into a 'carnival' or 'circus' and had not disrupted the 'judicial serenity and calm' to which Manafort was entitled.[22]

39.1.3 Trial and post-trial stage

Because the right to an impartial jury is also guaranteed by the US Constitution,[23] a defendant may question jurors about their exposure to pretrial publicity.[24] In one of the most highly publicised cases in modern history – the 1995 murder trial of football legend O J Simpson – it took nearly two months to seat an impartial jury not prejudiced by the near-constant media coverage of the case. During jury selection, jurors were prohibited from reading the papers, watching television or even awakening to a clock radio.[25] In the Manafort trial, Special Counsel Robert Mueller filed a motion to use a written juror questionnaire as a supplement for oral questions at jury selection to root out those jurors who might have formed biases or prejudged the evidence based on the extensive media coverage of the case.[26] Consistent with his claims of prejudice resulting from pretrial publicity in his motion to move his trial, Manafort agreed with the government's request to use a juror questionnaire as part of the jury selection. In widely publicised cases, courts frequently permit lawyers additional peremptory challenges (beyond the number normally allowed), which allow lawyers to summarily disqualify a potential juror without providing a reason to the court.[27] During the trial, jurors may be sequestered to protect them from the prejudicial effect of media reporting.[28] In this day and age, the court may instruct jurors not to read or post information about the trial on social media

22 *United States of America v. Manafort*, No. 1:18-cr-00083-TSE (E.D. Va. filed 17 Jul. 2018), ECF No. 138.

23 U.S. Const. amend. VI.

24 *United States v. Blanton*, 719 F.2d 815 (6th Cir. 1983) (holding that the court produced an impartial jury and fair trial by, at *voir dire*, through 'extensive questioning concerning prior media impact and juror associations, coupled with many dismissals based on even hints of possible prejudice, . . . very substantial increases in the number of peremptory challenges available to each defendant . . . [and] reliance on defendants' use of detailed questionnaires concerning all potential jurors coupled with sensitive responses by the court to any of defendants' challenges arising from such use').

25 http://law2.umkc.edu/faculty/projects/ftrials/Simpson/Simpsonchron.html.

26 *United States of America v. Manafort*, No. 1:18-cr-00083-TSE (E.D. Va. filed 21 Jun. 2018), ECF No. 87.

27 See, e.g., *United States v. Campa*, 459 F.3d 1121, 1135 (11th Cir. 2006) (noting that the district court twice granted the defendants' requests for additional peremptory challenges due to the publicity regarding the trial).

28 See, e.g., *United States v. Cacace*, 321 F. Supp. 2d 532, 536 (E.D.N.Y. 2004) (partly sequestering the jurors in a murder trial to reduce the risk that they may be prejudiced against the defendant, the acting boss of the Colombo crime family, by exposure to press reports of both charged and uncharged murders); *Geders v. United States*, 425 U.S. 80, 87 (1976). ('The judge's power to control the progress and, within the limits of the adversary system, the

© Law Business Research 2021

and other internet forums.[29] A failure to allow for a fair trial or to protect the impartiality of a jury will result in a mistrial and may require other post-trial remedies.[30] For example, the failure of a district court to adequately explore the impact of the extensive pretrial publicity in the 2015 trial of Dzhokhar Tsarnaev for the Boston Marathon bombings recently led the federal appellate court to vacate Mr Tsarnaev's death sentence. Specifically, the First Circuit Court of Appeals found that the lower court had not adequately assessed the impact of pretrial publicity on potential jurors, nor had it adequately investigated the potential jurors' use of social media expressing opinions about the case before and during trial. The court found that these errors resulted in a panel of jurors who had prejudged Mr Tsarnaev's guilt. The penalty portion of the case was remanded to the lower court for a retrial.[31] Prosecutors petitioned for Supreme Court review, however, and at the time of writing the Court had recently heard oral argument but no decision has been rendered. While the outcome of this particular case is therefore unclear, the potential impact of social media and other forms of publicity on jury trial remains a challenging issue for judges and parties alike.

Discovery of internal corporate communications 39.1.4

Issues of public access affect other areas of legal practice. Even where confidentiality of process and information is assumed, rules governing discovery in civil or criminal cases can lead to the disclosure of internal communications and records, even in sensitive investigations. The Federal Rules of Civil Procedure allow for pretrial discovery that is far more expansive compared to other jurisdictions.[32] Specifically, Rule 26(b)(1) allows parties to conduct discovery of 'any non-privileged matter that is relevant to any party's claim or defense and proportional to the needs of the case'.[33] As a result, companies that find themselves subject to class-action or shareholder derivative lawsuits that result from internal investigations are often forced to hand over troves of potentially

---

shape of the trial includes broad power to sequester witnesses before, during, and after their testimony.') The decision whether to sequester jurors is within the 'sound discretion' of the district court; e.g., *United States v. Porcaro*, 648 F.2d 753 (1st Cir. 1981).

29 See, e.g., *Bushmaker v. A. W. Chesterton Co.*, No. 09-CV-726-SLC, 2013 WL 11079371, at *12 (W.D. Wis. 1 Mar. 2013) (instructing the jury not to post on Twitter or Facebook); Judicial Conference Committee, Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate About a Case (Jun. 2012), available at www.uscourts.gov/file/18041/download.

30 e.g., *Pearson v. Rock*, No. 12-CV-3505, 2015 WL 4509610, at *2 (E.D.N.Y. 24 Jul. 2015) (granting a mistrial after concluding that the jury had been 'incurably tainted').

31 *United States of America v. Dzhokhar A. Tsarnaev*, No. 16-6001, 2020 WL 4381578 (1st Cir. 31 Jul. 2020).

32 See, e.g., Stephan N Subrin, 'Discovery in Global Perspective: Are We Nuts?', 52 *DePaul L. Rev.* 299 (2002).

33 Fed. R. Civ. P. 26(b)(1).

© Law Business Research 2021

damaging internal corporate communications. For example, the shareholder derivative litigation against the board of the Walt Disney Company lasted more than eight years, and the extensive discovery produced a damaging factual record about the board's corporate governance practices that ultimately forced Disney chief executive officer (CEO) and board member Michael Eisner to resign.[34] Although protective orders can limit disclosures to some extent during the discovery process, a presumption of public access arises once documents are filed in court in support of motions and as part of trial proceedings.[35]

See Chapter 11 on production of information to authorities

Civil discovery is not the only means through which seemingly confidential internal communications and records can become public. Many companies are forced to initiate or expand the scope of internal investigations after a regulator issues a subpoena or civil investigative demand for internal records. Additionally, certain public institutions, such as colleges and universities, are subject to public records laws that may require the institutions to release or publish documents both during and after the investigation.[36] And, increasingly, large-scale document leaks thrust internal corporate documents into the public sphere without warning.[37] The practical reality is that any organisation undergoing an internal investigation must prepare for the possibility that it will have to produce internal documents at some point.

Although a detailed description of all the defensive measures available to companies is beyond the scope of this chapter, a basic list should include confidentiality agreements to cover sensitive communications with third parties, protective orders (where available) to limit the scope and permitted usage of produced materials, and the careful maintenance of the attorney–client and work-product privilege during investigations.

See Chapter 37 on privilege

34 Érica Gorga and Michael Halberstam, 'Litigation Discovery and Corporate Governance: The Missing Story About the "Genius of American Corporate Law"', 63 *Emory L. J.* 1383, 1401–05 (2014).

35 *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986).

36 In 2014, after the University of North Carolina at Chapel Hill released a public report of an investigation into academic irregularities at the university, media organisations made requests through the North Carolina Public Records Law for the nearly 1.7 million electronic records that were collected and analysed during the investigation. The University of North Carolina at Chapel Hill, 'University reports final expenses to bring NCAA and related issues to a close' (13 Aug. 2018), http://carolinacommitment.unc.edu/updates/university-responds-to-public-records-requests-for-legal-communications-firm-expenses/.

37 For example, in 2007, an employee at HSBC Suisse surreptitiously downloaded client data from approximately 30,000 accounts and provided that data to French authorities. A portion of these files were then obtained through an international collaboration of news outlets and published in 2015 by the International Consortium of Investigative Journalists. See David Leigh et al., 'HSBC files show how Swiss bank helped clients dodge taxes and hide millions', *The Guardian* (8 Feb. 2015), https://www.theguardian.com/business/2015/feb/08/hsbc-files-expose-swiss-bank-clients-dodge-taxes-hide-millions?CMP=share_btn_tw.

© Law Business Research 2021

The effect of covid-19 on publicity of hearings and trials 39.1.5

As the covid-19 pandemic disrupted the world in 2020, courts were required to adapt to virtual hearings and trials. Remote hearings, available for the public to view from their homes, have brought transparency and increased scrutiny to proceedings that may have been ignored in the past. It is much easier to tune in to a virtual hearing on your laptop than travel to a courthouse. With increasing public access to the courtroom, issues of pretrial publicity or concerns about a litigant's public comments may soon be a quaint vestige of a bygone era. The public will be able to see and judge for themselves what is happening in a particular matter or trial. It may become harder to shape the public view by spinning the story.

However, increased public access is not always ideal. For example, whereas in a live trial setting a court or prosecutor can seek to exclude spectators who might threaten or intimidate a witness, there is no ability to control public access in a live stream. In recognition of that, the Pennsylvania Supreme Court recently halted live YouTube trial broadcasts.[38]

Consulting a public relations expert 39.1.6

Given the likelihood that the public may become aware of internal corporate communications relating to an investigation, many organisations (and some well-resourced individuals) resort to hiring a public relations expert to assist counsel during the course of an investigation. Public relations experts can serve a variety of functions, including preparing executives for public appearances during investigations, developing communications strategies around key investigation events (e.g., press conferences regarding investigation status), and planning for potential crises (e.g., a witness leaking the preliminary findings of an investigation prior to the investigation's completion). For many organisations, hiring a public relations expert to advise them during an internal investigation can be a foregone conclusion in the relentless 24-hour news cycle. Volkswagen, for example, hired three public relations firms based in three different countries to advise during its investigation of alleged emissions cheating.[39] During an investigation into potential corporate misconduct, special considerations arise when the public relations specialist works closely with legal counsel for the company. Frequently, questions of whether the attorney–client privilege applies to protect communications between lawyers and public relations experts arise during an investigation. Although the attorney–client privilege normally requires that the protected communication occur between a

38 Crime and Justice News, 'PA Supreme Court Halts Live YouTube Trial Broadcasts', The Crime Report (18 Sep. 2020), https://thecrimereport.org/2020/09/18/pa-supreme-court-halts-live-youtube-trial-broadcasts/.

39 Danny Hakim, 'VW's Crisis Strategy: Forward, Reverse, U-Turn', *N. Y. Times* (26 Feb. 2016), available at http://www.nytimes.com/2016/02/28/business/international/vws-crisis-strategy-forward-reverse-u-turn.html.

© Law Business Research 2021

lawyer and his or her client and exclude third parties, in some circumstances the privilege extends to communications between a non-lawyer consultant and the lawyer's client. In *United States v. Kovel*, for example, the Second Circuit held that communications between and among the client, the consultant and the attorney are privileged if they are made in confidence and 'for the purpose of obtaining legal advice'.[40]

Kovel, however, does not create a blanket privilege to protect communications between attorneys, their clients and public relations experts. Instead, after *Kovel*, courts determining whether to apply the attorney–client privilege to communications with consultants such as public relations experts have focused on whether the communications with the consultant were 'imparted in connection with the legal representation'.[41] For example, when Martha Stewart and her attorneys hired public relations consultants to assist them in dealing with the media in her high-profile insider trading case, the court protected those communications under the attorney–client privilege because the communications were made for the purpose of giving or receiving advice directed at handling Stewart's legal problems.[42] Applying *Kovel*, the court explained:

> *[T]his Court is persuaded that the ability of lawyers to perform some of their most fundamental client functions – such as (a) advising the client of the legal risks of speaking publicly and of the likely legal impact of possible alternative expressions, (b) seeking to avoid or narrow charges brought against the client, and (c) zealously seeking acquittal or vindication – would be undermined seriously if lawyers were not able to engage in frank discussions of facts and strategies with the lawyers' public relations consultants.*[43]

In contrast, the court in *Haugh v. Schroder Investment Management* found that the attorney–client privilege did not apply to a public relations expert retained for the plaintiff when the plaintiff could not show that the expert's services were 'anything other than standard public relations services' for the client, and were not necessary for plaintiff's counsel to provide the plaintiff with legal

40 296 F.2d 918, 922 (2d Cir. 1961) (protecting the communications from an accountant to the client that were made in confidence for the purpose of obtaining legal advice from the lawyer, not for the purpose of obtaining the accountant's advice).

41 *United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989).

42 *In re Grand Jury Subpoenas*, 265 F. Supp. 2d 321 (S.D.N.Y. 2003).

43 Id. at 330.

© Law Business Research 2021

advice.[44] The conclusion to be drawn from these two cases is simple.[45] To cloak communications with public relations experts advising clients in legal matters, the lawyer needs to retain the public relations expert, and the communications between the consultant and the client must be intended to assist the attorney in advising his or her client.

Social media and the press 39.2

Social media as an investigatory tool and as evidence 39.2.1

For better or for worse, social media is more than just a tool for friends and family to connect and communicate. The prevalence of social media has created a continuously updated record that is increasingly used to investigate wrongdoing and that can be admitted as evidence in judicial proceedings.

With respect to investigative activities, whether by the government or private parties, social media users generally do not have an expectation of privacy.[46] However, some of the typical features of social media – for example, the fact that social media users generally have password-protected accounts and various privacy settings to control what information other users can view – have created some legal distinctions. Courts have distinguished between public and non-public postings and focused on a user's privacy settings when determining whether Fourth Amendment protections against unreasonable searches extend to social media content accessed by the government.[47] However, even where a user limited viewable postings to his or her 'friend network', the government is not precluded from seeking co-operation from one of the user's friends authorised to view the user's content.[48] Unlike investigators, private American lawyers

---

44 No. 02-CIV- 7955, 2003 U.S. Dist. LEXIS 14586, at *8 (S.D.N.Y. 25 Aug. 2003) ('Plaintiff has not shown that Murray was "performing functions materially different from those that any ordinary public relations" advisor would perform.'); see also *Scott v. Chipotle Mexican Grill*, 94 F. Supp. 3d 585 (S.D.N.Y. 2015) (holding a factual report from a human resources consultant to employer's counsel was not protected by the attorney–client privilege because the employer did not show that it or counsel engaged consultant for anything more than factual research and to assist employer in making a business decision).

45 There is a circuit split as to how to handle these cases. Compare *NECA-IBEW Pension Tr. Fund v. Precision Castparts Corp.*, 2019 U.S. Dist. LEXIS 168088 (D. Or. 27 Sep. 2019) (denying plaintiff's motion to compel proxy documents sent from in-house counsel to employees of defence's public relations firm because the public relations firm was 'functionally an employee' of the defendant and the public relations firm was clearly receiving legal advice to guide its work), with *Universal Std. Inc. v. Target Corp.*, 331 F.R.D. 80 (S.D.N.Y. 6 May 2019) (sharing privileged communications with a public relations firm destroyed that privilege because the public relations firm was hired for business purposes, rather than to assist counsel in a legal task, the public relations firm did not improve counsel's understanding of the plaintiff's request for legal advice and an exception to waiver of the privilege was not found).

46 *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004).

47 See, e.g., *People v. Harris*, 949 N.Y.S.2d 590, 592 (N.Y. Crim. Ct. 2012).

48 See, e.g., *U.S. v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012).

© Law Business Research 2021

are constrained by ethical rules in their use of social media. For example, the New York State Bar Association's Committee on Professional Ethics has ruled that 'friending' an investigatory target or opposing party, or instructing a third party to do so on the lawyer's behalf, is a prohibited act of deceptive conduct or making of a false statement.[49] Accordingly, for private lawyers, care needs to be taken in how social media content is collected and used.

From the standpoint of admissibility as evidence in a proceeding, social media content is not fundamentally different from other paper or electronic evidence. The same evidentiary considerations apply: to be admissible, the evidence must be relevant, have probative value outweighing its potential to unfairly prejudice, and be authentic and free of hearsay.[50] Some courts treat evidence from social media similarly to other types of evidence and require only a threshold showing of authenticity.[51] Other courts require evidence that affirmatively disproves the possibility that evidence from social media was sent or manipulated by anyone other than its putative creator.[52]

39.2.2 Social media and the jury

In jury trials, issues surrounding social media generally fall into two categories: lawyers using social media to screen potential jurors, and jurors using social media improperly during a proceeding.

In the pretrial process, lawyers are ethically permitted to screen jurors based on social media profiles. On 24 April 2014, the American Bar Association issued Formal Opinion 466, which clarified that the act of passively observing a potential juror's public social media information is not improper *ex parte* contact with a juror or potential juror.[53] However, a lawyer may not send an invitation or request to friend or connect with a potential juror to gain access to the potential juror's information. Social media websites that provide notifications to users when their information is viewed, such as LinkedIn, also do not constitute improper contact as long as the lawyer does not make an active request to view non-public information.[54] If defence counsel learns from internet research that a prospective juror has made misrepresentations during *voir dire*, counsel should bring this misconduct to the court's attention. Failure

49 Robert H Giles and Jason I Allen, '"Will You Be My Friend?" – Ethical Concerns for Prosecutors and Social Media', Child Sexual Exploitation Program Update (National District Attorneys Association), 9 to 12 October 2012, at 2, available at http://www.ncdsv.org/images/NDAA-CSPE_WillYouBeMyFriend_2012.pdf.

50 See, generally, Fed. R. Evid. Authentication of evidence from social media is generally the biggest hurdle for admission, and two approaches are predominant.

51 See, e.g., *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

52 See, e.g., *Griffin v. Maryland*, 19 A.3d 415, 423–24 (Md. 2011).

53 ABA Comm. on Prof'l Ethics & Grievances, Formal Op. 466 (2014).

54 Id.

© Law Business Research 2021

to do so could potentially result in a waiver and an impairment of the defendant's right to an impartial jury.[55]

During trial, jurors' use of social media presents a risk of mistrial. To address this risk, counsel may request jury instructions on the use of social media prior to commencement of trial. Formal Opinion 466 also suggests that courts deliver jury instructions on the use of social media 'early and often' and even 'daily in lengthy trials'.[56] This guidance comes as jurors have used social media to publicly discuss trial issues or access witnesses and litigants, which ultimately has resulted in remands, reversals and other judicial inefficiencies.

For example, in *Dimas-Martinez v. State*, a death row inmate's murder conviction was reversed and remanded, in part because of a juror's tweets during trial.[57] The jury received instructions at the beginning of the trial warning them not to tweet or use social media but a juror nonetheless tweeted at the conclusion of the evidence in the sentencing phase of the trial.[58] The defendant's lawyer notified the court, and the court questioned the juror.[59] The juror admitted to the tweet and promised to discontinue use of social media for the duration of the trial.[60] But even though the juror tweeted at least two more times, the trial court refused a motion for a new trial, finding that the defendant suffered no prejudice from the tweets.[61] The Supreme Court of Arkansas disagreed, concluding that the juror's tweets were impermissible public discussion of the case, and that the insubordination of the juror to the court's instructions contributed to the defendant's denial of a fair trial.[62] In contrast, some courts have found that the use of social media alone is not necessarily prejudicial to the defendant if juror misconduct and actual prejudice are not found. For example, in *United States v. Aiyer*, the court found that a juror's mid-trial podcasts did not contain any evidence suggesting that the juror did not deliberate impartially. Having found that nothing in the podcasts suggested that the juror was biased against the defendant or that the defendant was prejudiced by the juror's podcasts, and that the audience of the podcast was too small to meaningfully prejudice the defendant, the court declined to conduct any post-verdict inquiries.[63]

55 See *United States v. Parse*, 789 F.3d 83, 114 (2d Cir. 2015) (holding that defence counsel did not knowingly waive the defendant's right to an impartial jury where, even though a Westlaw report indicated a juror may have in fact been a suspended attorney with the same name, the juror 'lied [so] comprehensively in *voir dire* and "presented herself as an entirely different person"' that defence counsel could have reasonably relied on her representations).

56 Id.

57 385 S.W.3d 238 (Ark. 2011).

58 Id. at 247–48.

59 Id. at 246.

60 Id. at 246–47.

61 Id. at 247.

62 Id. at 249.

63 *United States v. Aiyer*, 433 F. Supp. 3d 468, 477 (S.D.N.Y. 2020).

© Law Business Research 2021

The 2019 trial of Roger Stone, a confidant of President Trump, for making false statements to Congress and witness tampering, demonstrates issues that can arise when social media is used by the defendant prior to or during a trial. In Mr Stone's case, he routinely posted information about his case on Instagram. As a result of an Instagram photo of the judge presiding over his case with what appeared to be crosshairs in the background, the government sought to modify or revoke his pretrial bail status and to place strict limits on his right to speak publicly about the case. The Instagram post occurred just days after the court barred both counsel and Mr Stone from making statements to the media or the public that posed a threat of material prejudice to the case or that were intended to influence any juror, potential juror, judge or witness.[64] The court viewed the Instagram post as violating both its order on media comments and Mr Stone's bail conditions. The court prohibited Mr Stone from any media contact, prevented him from speaking or posting about the case anywhere and barred Stone from using surrogates to comment on his behalf about the case. Further, jurors in Mr Stone's case expressed fear after numerous tweets harassing and threatening the jury.[65] This unfortunate new trend demonstrates how social media has infiltrated the justice system. Social media has also been used to threaten judges and their families.[66] After a fatal attack on the family of US District Judge Esther Salas in July 2020, US courts requested Congress to pass legislation to protect disclosure of judges' personal information.[67] Finally, in the weeks leading to the US presidential election, the FBI arrested and charged 13 men with threatening to kidnap and kill the governor of Michigan in response to her strict social distancing and covid-19 related policies.[68]

39.3 Risks and rewards of publicity

39.3.1 Risks

High-profile criminal cases often generate media attention. And while courts may adopt judicial measures to limit the adverse effects of publicity, it may become so pervasive that it prejudices jurors' opinions regarding the question of guilt. In such cases, a court may declare a mistrial to protect the

64 *United States of America v. Stone*, No. 1:19-cr-00018-ABJ (.D.D.C.), ECF No. 36.

65 Zach Montague and Sharon LaFraniere, 'Judge in Roger Stone Case Warns About Attacks on Juror by Trump and Others', *N. Y. Times* (25 Feb. 2020), https://www.nytimes.com/2020/02/25/us/politics/roger-stone-jury-bias.html.

66 Ann E Marimow, 'Judges in D.C. Threatened, Harassed after High-profile, Political Legal Battles', *Washington Post* (18 September 2020), https://www.washingtonpost.com/local/legal-issues/judges-in-dc-threatened-harassed-after-high-profile-political-legal-battles/2020/09/18/acece6e2-f8e9-11ea-be57-d00bb9bc632d_story.html.

67 Todd Ruger, Federal Judges Want Safety Protections from Congress, Roll Call (15 Sep. 2020), https://www.rollcall.com/2020/09/15/federal-court-judges-safety-congress/.

68 Nicholas Bogel-Burroughs, Shalia Dewan and Kathleen Gray, 'F.B.I. Says Michigan Anti-Government Group Plotted to Kidnap Gov. Gretchen Witmer', *N. Y. Times* (8 Oct. 2020), https://www.nytimes.com/2020/10/08/us/gretchen-whitmer-michigan-militia.html.

© Law Business Research 2021

defendant's Sixth Amendment guarantee to have his or her case decided by an impartial jury.[69]

In other extraordinary situations, defence attorneys may face disciplinary measures – the most severe of which is disbarment – for improperly engaging the media in a manner that prejudices the proceedings.[70] Prosecutors are held to a higher standard than civilian attorneys under the professional rules.[71] For example, in June 2007, Michael B Nifong, the North Carolina prosecutor who pursued a false accusation of sexual assault against three Duke University lacrosse players, was disbarred by the State Bar Disciplinary Commission for making inflammatory statements to the media in violation of Rules 3.6 and 3.8(f) of the State Bar's Rules of Professional Conduct, among other violations.[72]

Unpopular defendants can face extraordinary difficulties in managing publicity while seeking an impartial hearing, which can increase both the cost and complexity of the defence. An example of this situation is the prosecution of Martin Shkreli, a former pharmaceutical CEO and hedge fund manager who was convicted of securities and wire fraud violations stemming from losses suffered by investors in his funds and companies.[73] As the CEO of Turing Pharmaceuticals, Mr Shkreli unapologetically raised the price of a life-saving drug by 5,000 per cent[74] and became known in the media as 'the most hated man in America'.[75] Mr Shkreli's notoriety generated daily news coverage of his subsequent federal trial which, combined with his ill-advised attempts to personally manage the publicity, required the trial judge to issue orders addressing the media's and Mr Shkreli's potential influence on the jury.[76]

---

69 See *Sheppard*, 384 U.S. at 363; see also *Arizona v. Washington*, 434 U.S. 497, 505–06 (1978) (mistrial is reserved for those special cases in which there is a 'manifest necessity').

70 See, e.g., Model Rules of Prof'l Conduct R. 3.6 (Trial Publicity) (prohibiting a lawyer from making an 'extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter').

71 See, e.g., Model Rules of Prof'l Conduct R. 3.8(f) (Special Responsibilities of a Prosecutor) (prohibiting a prosecutor from making extrajudicial comments that have a 'substantial likelihood of heightening public condemnation of the accused').

72 Id.

73 Superseding Indictment, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 3 Jun. 2016), ECF No. 60.

74 Andrew Pollack, 'Drug Goes from $13.50 a Tablet to $750, Overnight', *N. Y. Times* (20 Sep. 2015), available at https://www.nytimes.com/2015/09/21/business/a-huge-overnight-increase-in-a-drugs-price-raises-protests.html.

75 Phil McCausland, 'Fraud Trial for Martin Shkreli, "Most Hated Man in America", Begins Monday', *NBC News* (25 Jun. 2017), available at https://www.nbcnews.com/news/us-news/fraud-trial-martin-shkreli-most-hated-man-america-begins-monday-n776581.

76 Docket Order, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 5 Jul. 2017) (following Mr Shkreli's courthouse visit with reporters covering his trial, when he remarked on evidence and the credibility of a witness, prosecutors moved for a gag order to prohibit Mr Shkreli

© Law Business Research 2021

Mr Shkreli was convicted on two counts of securities fraud and one count of conspiracy to commit securities fraud.[77]

Civil defamation claims may also follow highly publicised cases. When numerous women accused actor and comedian Bill Cosby of sexual assault, Mr Cosby and his team publicly denied the allegations and accused the women of lying.[78] Several of the alleged victims filed civil defamation suits against Mr Cosby. A federal judge in Pennsylvania dismissed one of the suits on the basis that Mr Cosby's statements did not support a claim for defamation under state law,[79] while Mr Cosby settled a defamation suit that was pending in federal court in Massachusetts.[80]

39.3.2 Rewards

When properly executed, tactical media coverage during an investigation or trial can counter negative public impression and alleviate prosecutorial pressure to bring charges. The public relations consultants hired by Martha Stewart in connection with her insider trading case focused narrowly on neutralising the media coverage that reached the prosecutors and regulators responsible for charging decisions so that they could make their decisions without 'undue influence from the negative press coverage'.[81] In ruling on the attorney–client privilege afforded to certain communications among Stewart, her attorneys and the public relations firm, the Court recognised the necessity of developing a communications plan in high-profile cases:

> *Just as an attorney may recommend a plea bargain or civil settlement . . . so too an attorney may take reasonable steps to defend a client's reputation and reduce the adverse consequences of indictment. . . . A defense attorney may pursue lawful strategies to obtain dismissal of an indictment or reduction of charges, including an attempt to demonstrate in the court of public opinion that the client does not deserve to be tried.*[82]

Given the importance of advocating outside the courtroom, it may also be beneficial for an attorney to exercise the right to reply under the Model Rules

---

from making any public statements about the case. Two days later, the court issued a limited gag order prohibiting Mr Shkreli from making 'comments to the press regarding the case, evidence or witnesses within the courthouse or the courthouse perimeter').

77 Verdict, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 4 Aug. 2017), ECF No. 305.

78 See Mike Nunez, 'Bill Cosby to FLORIDA TODAY: I won't mention allegations', *Florida Today* (22 Nov. 2014), available at http://www.floridatoday.com/story/news/local/2014/11/21/bill-cosby-to-florida-today-i-wont-mention-allegations/19367957/.

79 *Hill v. Cosby*, No. 15-1658, 2016 U.S. Dist. LEXIS 7300 (W.D. Pa. 21 Jan. 2016).

80 *Green v. Cosby*, No. 3:14-cv-30211 (D. Mass. filed 10 Dec. 2014).

81 *In re Grand Jury Subpoena*, 265 F. Supp. 2d at 323–24.

82 Id. (quoting *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1043 (1991) (Kennedy, J, plurality opinion)).

© Law Business Research 2021

of Professional Conduct. Notwithstanding the prohibition at Rule 3.6(a) against extrajudicial statements that are substantially likely to materially prejudice a fair trial, Rule 3.6(c) permits a lawyer to make extrajudicial statements that protect a client from the 'substantial undue prejudicial effect' of recent publicity that was not initiated by the lawyer or the client to the extent that they are necessary to mitigate the adverse publicity.

© Law Business Research 2021

40

Data Protection in Investigations

Stuart Alford QC, Serrin A Turner, Gail E Crawford, Hayley Pizzey, Mair Williams and Matthew Valenti[1]

40.1 Introduction

Data protection law is a misleading term, because the relevant framework will be a combination of employment, whistleblower, criminal and privacy laws. Companies and practitioners must navigate domestic and international legislation that touches on data protection, while ensuring they stay on the right side of regulatory and prosecuting agencies and co-operate with them to the extent that it is of benefit.

Handling data about individuals has become increasingly complex, particularly when the data protection regimes in different jurisdictions appear to impose conflicting obligations on data holders.

This chapter will look at both UK (including some European) and US laws and how they frame issues around investigations and data protection. We will look at internal investigations and those conducted by authorities, and provide some specific guidance in respect of data protection and whistleblowing regimes.

In the United Kingdom, a balance must be struck between compliance and regulatory obligations that require the processing of data as part of investigations, and the protection afforded to individuals caught up in those investigations, primarily under the UK General Data Protection Regulation[2] (UK

1 Stuart Alford QC, Serrin A Turner and Gail E Crawford are partners, and Hayley Pizzey, Mair Williams and Matthew Valenti are associates, at Latham & Watkins.

2 UK GDPR, available at https://www.legislation.gov.uk/eur/2016/679/contents; Keeling schedules for the UK GDPR and the DPA 2018, which show the changes made post-Brexit, are available at https://www.gov.uk/government/publications/data-protection-law-eu-exit.

© Law Business Research 2021

GDPR), which effectively retains Regulation (EU) 2016/679 (EU GDPR)[3] in UK law following the end of the Brexit transition period, and the UK Data Protection Act 2018 (DPA 2018).[4] In September 2021, the UK government opened a public consultation on wide-ranging reform to UK data protection laws, including proposals for an expansive framework for international data transfers.[5] The consultation closed in November 2021; further policy and regulatory developments are expected as the proposed reforms take shape.

UK laws governing the interception and monitoring of communications may also require navigation in internal investigations. Although legislation protecting individuals' data has existed for years, the increased sanctions for breaches under the GDPR (maximum fines being the higher of £17.5 million/€20 million or up to 4 per cent of annual worldwide turnover), and increased regulatory focus on data privacy, mean that investigators must take the protections afforded to individuals more seriously than they did previously. Across Europe, the GDPR largely consolidated and harmonised the previous European data protection regime, but it does not necessarily simplify the issue between Member States. Each Member State may have its own laws in place as long as the basic standards of the GDPR are met; the GDPR is a floor and not a ceiling.

Furthermore, both the UK GDPR and the EU GDPR catch not only UK/EU corporations and global company groups with a UK/EU presence (including their use of personal data outside the UK/EU to the extent that use is intrinsically linked with their domestic activities), but also affect any corporations overseas and with no UK/EU presence that actively offer goods and services to, or monitor the behaviour of, individuals within the UK/EU, even if the data is stored overseas. Multinational organisations may be required to comply with both the EU GDPR and the UK GDPR, depending on the scope of the investigation in question.

In the United States, there is no uniform, omnibus federal privacy regime comparable to the GDPR. However, a patchwork of federal and state privacy laws may come into play in an internal investigation, particularly when reviewing and collecting employees' electronic communications. To minimise legal risk, companies should provide employees with clear notice that their electronic communications stored on company systems or devices are subject to monitoring and search.

Given the territorial reach of both the UK GDPR and the EU GDPR, US and multinational companies may have to grapple with both sets of compliance obligations in conducting an internal investigation or responding to criminal

3 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

4 DPA 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

5 Data: A new direction (10 September 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

© Law Business Research 2021

or regulatory investigations. Where a US or multinational company's obligations to comply with US legal demands for personal data conflict with GDPR limits on the processing and transfer of that data to the United States, the company must assess whether it can lawfully transfer responsive data to the United States that is subject to the UK GDPR or EU GDPR, or both. This assessment is all the more important, and complex, in light of the Court of Justice of the European Union's (CJEU) decision in *Schrems II* (applicable in the United Kingdom and the European Union).[6] That decision invalidated the EU-US Privacy Shield (the framework designed to regulate the exchange of personal data from organisations in the EU to Privacy Shield-certified organisations in the United States), and imposed a number of caveats on the use of the standard contractual clauses (SCCs) (an alternative to the EU–US Privacy Shield as a data transfer mechanism) to transfer personal data to the United States. If the US or multinational company cannot lawfully transfer responsive data to the United States, it may need to negotiate with the requesting legal authority to narrow the scope of the request or to develop other ways of resolving the legal conflict. Where the conflict cannot be resolved, the US or multinational company may need to consider challenging the request on comity grounds, although such challenges have rarely succeeded in criminal or regulatory investigations.[7]

40.2 Internal investigations: UK perspective

Internal investigations will inevitably deal with personal data, particularly employees' data, which in the United Kingdom is governed by the UK GDPR and DPA 2018. For those conducting internal investigations, the key obligations to consider are:

- transparency, namely the requirement to inform individuals about how their personal data is being used (unless there is a relevant exemption);
- data minimisation, namely the requirement to ensure that use of personal data for the investigation is proportionate;
- establishing a legal basis for the processing of personal data, as prescribed by the UK GDPR (consent and legitimate interest are two of the legal bases companies and practitioners can commonly rely on to process data in an internal investigation);

6 *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (Case C-311/1).

7 See *In re Grand Jury Subpoena dated Aug. 9, 2000*, 218 F. Supp. 2d 544, 554 (S.D.N.Y. 2002) ('Courts consistently hold that the United States interest in law enforcement outweighs the interests of the foreign states in bank secrecy and the hardships imposed on the entity subject to compliance.') (collecting cases); see also *In re Grand Jury Proceedings*, 532 F.2d 404 (5th Cir.), cert. denied, 429 U.S. 940 (upholding grand jury subpoena against comity challenge based on foreign banking privacy laws).

© Law Business Research 2021

- if applicable, establishing a relevant condition on which to process any 'special categories' of personal data or any criminal offences data involved (in addition to a legal basis for the processing), and;
- if personal data will be transferred, or accessed from, outside the United Kingdom, ensuring a legal basis for that data transfer, as prescribed by the UK GDPR (in addition to a legal basis for the underlying processing).

Transparency 40.2.1

The UK GDPR and DPA 2018 require relevant organisations to inform individuals in advance about how their personal data is processed, in a clear and accessible manner, and prescribe the minimum information to be provided.[8] Meeting these obligations in internal investigations can present practical challenges if an organisation does not have a comprehensive monitoring policy, as use of employees' personal data for investigation purposes may well be detrimental to, and unexpected by, those employees.

There are certain exemptions under the DPA 2018 to the specific obligation to provide minimum information to individuals. When collecting personal data directly from an individual, organisations need not provide data protection information that the individual already has. This may be relevant for organisations conducting investigations into, or involving, their employees and using personal data the organisation has obtained from them, if the organisation already provides some level of privacy information to them. A wider range of exemptions are available in circumstances where the personal data is obtained from other sources. The most relevant exemptions in internal investigations apply if providing the information to the individual would be impossible or would involve disproportionate effort, or would render impossible or seriously impair achievement of the objectives of the processing; or the organisation is required by law to obtain or disclose the personal data (under a binding legal obligation, rather than, for example, compliance with a non-binding code of practice, an informal, non-binding regulator request or a contractual obligation).

In addition to the transparency principles under the UK GDPR, the United Kingdom's regulatory framework for communications monitoring also requires organisations to be transparent with employees about the interception and monitoring of their communications (in written policies and in consistent business practices). Taken together, in internal investigations, the data protection and communications regimes oblige organisations to be clear and open with employees about how their personal data and communications are used, and to ensure that any interception and subsequent review, use and disclosure of data and communications in an investigation is lawful and proportionate. Robust, clear and accessible data privacy information notices for employees,

8 This minimum information includes, among other things, the purposes of the processing, the lawful basis for the processing, the recipients or categories of recipients of the personal data, details of data transfers outside the United Kingdom and applicable data retention periods.

© Law Business Research 2021

and policies on employee monitoring, will provide a valuable shield against claims of employee privacy infringement and non-compliant monitoring practices – at least in the United Kingdom.[9]

40.2.2 Data minimisation

The UK GDPR principle of data minimisation should be applied by organisations across their personal data activities generally, including internal (and external) investigations. Organisations should ensure that the collation, review, use and disclosure of individuals' data during the investigation is proportionate and no more intrusive than is necessary to achieve the legitimate purposes of the investigation. This will be relatively straightforward for clearly defined and focused investigations, but may prove more challenging to assess in practice in wide-ranging investigations requiring significant levels of data for loosely defined purposes. Organisations would be well advised to document the investigation's scope and associated personal data proportionality assessment, to demonstrate that data minimisation principles have been applied. Practical safeguards to ensure proportionality should also be applied, such as appropriately limiting the scope of documentation, email and communications review and disclosure (limiting impacted custodians and individuals, using keyword searches and time periods to identify relevant information, etc.).

40.2.3 Legal basis for data processing: consent

Consent from individuals provides a legal basis for the processing of their personal data, provided the UK GDPR consent conditions are met. Consent must be given freely and clearly, and in plain language, and must be an affirmative act – consent cannot be given by inactivity, such as pre-ticked boxes in an online form.[10]

In the typical employer–employee context of an internal investigation, the concept of consent being freely given is complicated. Given the dynamic, some jurisdictions consider that consent from an employee to an employer may never be freely given,[11] a position exacerbated in an internal investigation by the added element of potential wrongdoing by the employee or another individual, and tipping-off considerations. Investigators should ensure they comply

9 The position in a number of European jurisdictions (including France and Germany) is considerably more protective of employee rights and restrictive of an employer's ability to intercept or review communications or to access employee devices.

10 UK GDPR, Article 7 and Recital 32.

11 The European Data Protection Board's (EDPB) Guidelines on consent under the EU GDPR deem reliance on consent to be 'problematic' in an employment context, and recommends that it is not relied on other than in exceptional circumstances. Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020), at p. 9, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. The UK Information Commissioner's Office (ICO) considers that the EDPB's guidelines and opinions may offer guidance in applying the UK GDPR, in the absence of UK-specific guidance or regulations.

© Law Business Research 2021

with the UK GDPR, either by getting express consent from the data subject to process their data, which may not be feasible in an internal investigation if it cannot be considered freely given or because the organisation does not want to notify the individual of the investigation (blanket clauses in employment contracts will no longer be enough), or by relying on another lawful basis under the UK GDPR to lawfully process the data.

Legal basis for data processing: legitimate interest 40.2.4

The UK GDPR provides a number of other legal bases for the processing of personal data in certain circumstances.[12]

Under the UK GDPR, an organisation can consider the legitimate interests of a third party or public interest, as well as its own legitimate interests, when assessing the use and processing of personal data.

In an internal investigation, this ability could allow an organisation to rely on the lawful basis of legitimate interests (of a third party or public interest) to process personal data. The rights of individuals can, however, override a legitimate interest, if the effect on an individual's interests or fundamental rights override the organisation's (or a third party's) legitimate interests.

The Information Commissioner's Office (ICO) enforces data protection legislation and has stated: 'Legitimate interests is the most flexible lawful basis for processing.' The ICO has set out a three-part, cumulative test for establishing whether there is a legitimate interest in processing the data, which may be a useful addition to an investigation plan:

- Purpose test: is the purpose of the processing a legitimate interest?
- Necessity test: is the processing of the data necessary and proportionate for the purpose?
- Balancing test: is the legitimate interest overridden by the individual's interests, rights and freedoms?[13]

The above test can be used by those conducting internal investigations to justify the processing of data under the UK GDPR because it is for the legitimate purpose of the company itself, or a third party, provided any risk of undue harm to the individual does not outweigh that interest.[14] In respect of the necessity test, companies must consider whether there is an alternative, less intrusive, means of gathering or processing the same information.

12 UK GDPR, Article 6.

13 'Legitimate interests' (ICO), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

14 The UK government's proposed data protection reforms include a proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. The proposed list includes the following interests that may be relevant in investigations: the reporting of criminal acts to appropriate authorities; and improving or reviewing an organisation's system or network security. The government is seeking views on both the creation of a list and on the interests and activities to be included.

© Law Business Research 2021

To demonstrate compliance with the UK GDPR, organisations will have to document their decisions carefully (through a legitimate interests assessment).[15]

40.2.5 Special category and criminal offences data

When processing data in an internal investigation, data controllers must pay increased attention when dealing with special category data.[16] In an internal investigation, this kind of information will often be held in a human-resources file that becomes part of a review within the investigation. Employee emails or instant messages, etc., could possibly be considered special category data, as they could potentially contain data within this definition. However, it is certainly arguable that emails should not fall into this category on the basis that any special category data is incidental and not part of the primary purpose of the use of data in that context. This argument is strengthened by the application of data minimisation steps to ensure the special category data is not specifically identified or targeted as part of the investigation.

When dealing with special category data, organisations must establish both a legal basis for the data processing (e.g., consent, legitimate interests or another basis under the UK GDPR) and an additional, specific legal basis for processing the relevant special category data. The UK GDPR and DPA 2018 provide for a number of specific legal bases or conditions for the use of special category data.[17]

Information about criminal allegations, proceedings or convictions in relation to an individual may also be relevant in an internal investigation. This data is treated separately to special category data under the UK GDPR, and requires a lawful basis for processing and legal or official authority to handle that data, which must be prescribed under national law. In the United Kingdom, the UK GDPR and DPA 2018 authorise the processing of criminal offences data in limited circumstances and subject to the conditions set out in the UK GDPR and DPA 2018.[18] These legal authority grounds are narrow, though some may be available in internal investigations, including prescribed public interest grounds, consent of the individual and establishing or defending a legal claim. Special category data and criminal convictions data should be handled with particular consideration, and organisations should ensure that the basis on which they are using this data is clearly documented.

15 ibid.

16 Special category data is defined in the UK GDPR and the DPA 2018 as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (UK GDPR, Article 9; DPA 2018, s.10).

17 UK GDPR, Article 9; DPA 2018, ss.10 and 11 and Schedule 1.

18 UK GDPR, Article 10; DPA 2018, ss.10 and 11 and Schedule 1.

© Law Business Research 2021

Public interest 40.2.6

The public interest ground for processing special category or criminal offences data may be useful in an internal investigation, especially where it is likely to be followed by a regulatory investigation, and where consent or another legal basis is not available in practice. This ground is limited to those public interest purposes that are specifically provided for in national law. Under the DPA 2018, these public interest purposes are relatively narrowly defined, meaning this ground will be difficult to satisfy in practice, and organisations should be confident in, and have clearly documented, their justifications before relying on this basis.

Under the DPA 2018, the public interest purposes of particular relevance to internal investigations relate to the prevention or detection of unlawful acts, and to protecting the public against dishonesty, in both cases provided there is also a 'substantial public interest'.[19] Both provisions require that processing be done without consent of the individual, to avoid prejudicing the investigation. As the scope of the public interest ground for data processing (under the EU GDPR as well as the UK GDPR) must be provided for under national law, it may vary across the European Union. Organisations should therefore seek local legal advice in the relevant Member States.

Data transfer outside United Kingdom and European Economic Area 40.2.7

Given the international scope of many investigations, companies should consider the practicalities of exporting data while complying with the UK GDPR and the EU GDPR (as applicable). If the personal data will be transferred, or accessed from, outside the UK or European Economic Area (EEA) – whether from within the organisation's corporate group or externally – that data transfer also requires a separate lawful basis under the UK GDPR or EU GDPR, in addition to the lawful processing of the data itself. This restriction on data transfers does not apply to third countries recognised as 'adequate' by the UK Secretary of State or the European Commission respectively, to which personal data may be transferred freely.[20] Following Brexit, relevant adequacy decisions have been passed by the European and UK authorities to permit the unrestricted transfer of personal data between the EEA and the United Kingdom.

On 16 July 2020, in the *Schrems II* decision, the CJEU invalidated the European Commission's EU–US Privacy Shield Adequacy Decision

19 DPA 2018, Schedule 1, Part 2.

20 For transfers under the EU GDPR, the European Commission has recognised the following countries as having adequate protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, United Kingdom and Uruguay. An adequacy decision in relation to South Korea is being adopted. For transfers under the UK GDPR, the UK Secretary of State has recognised the following countries as having adequate protection: all EEA jurisdictions, Gibraltar and jurisdictions recognised as adequate by the European Commission, as at 31 December 2021.

© Law Business Research 2021

(2016/1250), one of the key mechanisms for lawfully transferring personal data from the EEA to Privacy Shield-certified organisations in the United States, on the basis that the Privacy Shield did not provide an 'adequate' level of protection required under the GDPR for the transfer of data from the EEA to the United States.[21] In the same judgment, the CJEU ruled that SCCs[22] remain valid in respect of any personal data export (not just EEA–US transfers), but imposed caveats on their use.

The data transfer safeguard most commonly relied on in investigations, for intra-group transfers within an organisation or to or from third-party providers involved in the investigation, consists of using SCCs. These are European Commission approved standard-form contractual agreements that put in place binding data protection obligations between the data exporting and importing entities. On 4 June 2021, the European Commission issued revised SCCs for data transfers subject to the EU GDPR,[23] which replace the previous SCCs from 27 September 2021 (though contracts under the previous SCCs in place on this date may be relied on until 27 December 2022, by when all previous SCCs must be migrated to the revised SCCs). The revised SCCs are not recognised for data transfers subject to the UK GDPR, for which organisations should continue to rely on the previous SCCs, until the ICO's revised data transfer mechanisms under the UK GDPR are in effect.[24]

Following the *Schrems II* decision, organisations seeking to rely on the SCCs, for data transfers subject to the UK GDPR or the EU GDPR and pursuant to the revised or the previous SCCs, must assess, case by case, whether the law of the destination country ensures adequate protection for the personal data being transferred, and to put in place supplementary measures to ensure an essentially equivalent level of protection if required.[25] In relation to data transfers to the United States specifically, the CJEU found that, in its judgment and in the context of the Privacy Shield, the US legal regime does not ensure

21 *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (Case C-311/1).

22 Sometimes referred to as the 'Model Clauses'.

23 Available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

24 On 11 August 2021, the ICO opened a consultation on its proposed, revised data transfer package under the UK GDPR, which includes an International Data Transfer Agreement to replace the previous SCCs, and a UK Addendum to the revised SCCs intended to allow the revised SCCs to be used for data transfers under the UK GDPR.

25 The EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en) set out the EDPB's recommendations and guidance on how the required assessment may be carried out and provides of examples of potential supplementary measures. The ICO's proposed data transfer package includes an international transfer risk assessment and tool, which provides guidance and a framework for conducting the required assessment for UK GDPR transfers.

© Law Business Research 2021

an essentially equivalent level of protection. The CJEU was particularly focused on access rights to data by US public authorities for national security purposes, and associated individual rights and remedies. In light of the evolving SCCs requirements and enforcement landscape in practice, organisations should carefully consider use of the SCCs to validate data transfers to the United States in internal investigations, whether under the EU GDPR or the UK GDPR, and document any data transfer assessments and any supplementary measures.

There are alternatives to the SCCs, though they may not be as reliable in practice for organisations conducting investigations. This includes the explicit consent of the individuals, and transfers required to establish or defend a legal claim (applicable for occasional transfers only).

Different data transfer considerations apply in investigations by authorities.

Third parties to investigations 40.2.8

Companies and practitioners often rely on third parties to assist with internal investigations (for example, in data analysis, legal advice or document review). These third parties will often need access to personal data. The UK GDPR requires that a contract (or equivalent legal act) is put in place where controllers engage the services of processors.

This contract must set out, among other information, the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, as well as prescribed contractual obligations, including an obligation of confidentiality.[26]

Monitoring employees' electronic communications 40.2.9

A framework of regulations is in place in the United Kingdom to govern the extent to which employers can intercept and monitor their employees' electronic communications.[27] These communications regulations are triggered upon 'interception' of communications, defined as making the content of the communication available to a person who is not the sender or intended recipient, whether before, during or after transmission of the communication. In internal investigations, this will most likely be relevant when considering investigation-specific interception and monitoring of employee communications, or when assessing the legality of an organisation's communications monitoring practices.

The default position is that employers may not intercept employee communications other than with the consent of both the sender and the recipient of

26 UK GDPR, Article 28(3).

27 This framework consists primarily of the Investigatory Powers Act 2016 (IPA 2016); the Interception of Communications Code of Practice under the IPA 2016; and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (Business Interception Regulations) enacted under the IPA 2016.

© Law Business Research 2021

the communication, or as authorised by the exemptions built into the legal framework. In practice, organisations carrying out internal investigations are most likely to rely on exemptions that permit interception: to monitor employee or external users' compliance with rules governing use of the system (whether internal policies or legal or regulatory requirements); to maintain records and establish facts; to prevent or detect crime; or for information security purposes.[28] If consent is relied on for interception purposes, this should be distinguishable from any consent relied on for UK GDPR purposes (which sets a higher consent standard), so that both interception and data protection consents can be evidenced if required.

40.3 Internal investigations: US perspective

The United States has no single unified data protection regime. However, a patchwork of federal and state privacy laws impose various constraints on the extent to which a company may collect and review information about its employees, particularly their electronic communications.

State privacy laws in the United States vary considerably, but many states recognise a common-law right against unreasonable intrusions into a person's seclusion or privacy. Such causes of action have arisen against employers following searches in the workplace.[29] Accordingly, companies are well advised to have written policies, that all employees must acknowledge, clearly providing that the company's network and systems are subject to monitoring and search.

Other state laws place more specific prohibitions on employers that can limit the outer bounds of a company's investigative actions, for example prohibiting questioning an employee on issues that serve no business purpose,[30] or demanding an employee disclose passwords and other credentials to personal email and social networking accounts.[31]

Various state and federal laws also restrict the collection of electronic communications, including emails (work and personal), phone calls[32] and social

28 Provided for under the Business Interception Regulations and the Interception of Communications Code of Practice.

29 See, e.g., *Rowe v. Guardian Auto. Prods*., 2005 WL 3299766 (N.D. Ohio 6 December 2005); Restatement (Third) of Emp't Law: Emp't Privacy & Autonomy ch. 7 (Council Draft No. 6, 2011), available at http://extranet.ali.org/docs/Employment_Law_CD6_online.pdf (introducing the tort of wrongful employer intrusion upon a protected employee privacy interest and stating that '[e]mployees have a right of privacy against wrongful employer intrusions upon protected employee privacy interests' including personal information').

30 See 2 Cal. Code Regs. § 7286.7(b) (prohibits employers from inquiring into any issues that otherwise serve no 'business purpose').

31 See, e.g., Cal. Labor Code § 980.

32 Some states require the consent of all parties to legally record a phone call. See, e.g., Cal. Penal Code § 630 et seq. (2006); Conn. Gen. Stat. § 52-570d (2006); Fla. Stat. §§ 934.01 to .03 (2005); 720 Ill. Comp. Stat. 5/14-1, -2 (2006); Md. Code Ann. Cts. & Jud. Proc. § 10-402 (2006); Mass. Gen. Laws ch. 272, § 99 (2006); Mont. Code Ann. 45-8-213; N.H. Rev Stat. Ann. §§ 570-A:l,

© Law Business Research 2021

media accounts.[33] One primary federal law is the Electronic Communications Privacy Act,[34] which breaks down into the Wiretap Act (regulating interception of electronic communications),[35] the Pen Register Statute (regulating use of a pen register to track communications)[36] and the Stored Communications Act (regulating unauthorised access to stored electronic communications).[37] These statutes do not generally prohibit an employer from searching its own email system.[38] However, they may limit an employer's ability to use company-owned equipment to access an employee's communications stored with third-party providers (e.g., Gmail),[39] at least without the employee's consent. Other state laws govern an employer's ability to collect and use biometric data like fingerprints, voice prints or vein patterns from employees. One such law is the Illinois Biometric Information Privacy Act, which requires informed written consent prior to collection of biometric information.[40]

Finally, besides state and federal laws, internal investigations in the United States may also be subject to extraterritorial GDPR restrictions. In particular,

---

570-A:2 (2005), as amended by New Hampshire Laws Ch. 169 (H.B. 1353) (2016); 18 Pa. Cons. Stat. § 5701 et seq. (2005); Wash. Rev. Code § 9.73.030 (2006). Other states require just one party consent. See, e.g., Ariz. Rev. Stat. Ann. § 13-3005; D.C. Code Ann. § 23-542(b)(3); N.Y. Penal Law § 250.00(1); N.J. Rev. Stat. § 2A:156A-4(d); Ohio Rev. Code Ann. § 2933.52(B)(4); Tex. Penal Code Ann. § 16.D2(c)(4).

33 See, e.g., Cal. Lab. Code § 980; 19 Del. Code § 709A(b); Md. Code Lab. & Empl. § 3-712(b)(1); Nev. Rev. Stat. § 613.135; N.H. Rev. Stat. § 275:74; 820 Ill. Comp. Stat. § 55/10(b)(1).

34 See 18 U.S.C. §§ 2510-22, 2701-12.

35 Id., at §§ 2511–2522.

36 Id., at §§ 3121–3127.

37 Id., at §§ 2701–2711.

38 Id., at § 2701; see, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (holding that the insurance company that leased a computer system to an agent did not violate the Electronic Communications Privacy Act (ECPA) when it retrieved stored emails from computers); see also *Scott v. Beth Israel Med. Ctr., Inc.,* 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007) (holding that a policy that employees had no privacy right over material created, received, saved, or sent using the employer's computer system sufficient to eliminate any expectation of privacy); *United States v. Etkin*, 2008 U.S. Dist. LEXIS 12834, at *14 to 16 (S.D.N.Y. 20 February 2008) (employees do not have a reasonable expectation of privacy when employers warn the employees via log-on notices or flash-screen warnings of a policy through which the employer could monitor or inspect the computers at any time); *United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002) (holding no reasonable expectation of privacy where an employer's policy 'clearly warned computer users [that] data [wa]s "fairly easy to access by third parties"'); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (holding that any reasonable expectation of privacy employee had in his work computer was eliminated when the employer announced that it could inspect the computer).

39 See 18 U.S.C. § 2701(a); see, e.g., *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 757, 758 (N.D. Ohio 2013) (denying an employer's motion to dismiss claims under the ECPA where an employee alleged that her supervisor accessed unopened emails from her Gmail account through her employer-issued BlackBerry).

40 740 ILCS 14/1 (2008); id., at § 10.

© Law Business Research 2021

to the extent the investigation requires review of personal data stored in the United Kingdom or European Union – for example, an employment file for an employee in a UK or EU affiliate, stored locally – then the company must evaluate whether (1) the affiliate has a legal basis on which to disclose the data to the United States, (2) transparency obligations have been met and relevant information or notices have been provided (or an exemption applies), (3) data minimisation and proportionality principles have been applied and (4) one of the conditions for the transfer of personal data to the United States has been met. If the organisation cannot meet the requirement to legitimise the transfer, the company may wish to consider ways of handling the data that do not involve transferring personal data to the United States – such as reviewing the relevant personal data in the United Kingdom or European Union, or redacting personal information from the data set before it is transferred.

40.4 Investigations by authorities: UK perspective

Companies have always had to consider competing interests when dealing with investigating authorities, but, data protection has, historically, rarely been near the top of any list of considerations. The very significant fines available under the UK GDPR mean that companies must take data protection much more seriously, particularly the disclosing of personal data to authorities in the United Kingdom and overseas. The ICO has shown that it will not hesitate to use its powers under the UK GDPR to investigate and issue significant fines for breaches. In October 2020, the ICO fined British Airways £20 million for failing to protect the personal and financial details of more than 400,000 of its customers impacted by a data breach.[41] Later the same month, the ICO fined Marriott International Inc £18.4 million for infringements of the GDPR stemming from a data breach at Starwood, which Marriott acquired in 2016, affecting millions of individuals.[42] Although these represent a reduction of nearly 90 per cent and 81 per cent, respectively, from the originally proposed fines, the British Airways fine represents the largest fine imposed by the ICO to date for breach of the GDPR. It remains to be seen whether this initially robust approach to UK GDPR enforcement from the ICO will extend into the more nuanced environment of internal and regulatory investigations, with their frequently competing legal obligations. Moreover, following Brexit, organisations managing investigations that span the United Kingdom and European Union may be subject to, and exposed to enforcement under, both the UK GDPR and the EU GDPR.

41 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

42 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data- secure/.

© Law Business Research 2021

Providing data to authorities 40.4.1

Where authorities make requests for data, companies must be absolutely clear about the legal powers by which those requests are being made, to ensure that they can comply with the request while fulfilling their UK GDPR obligations. The benefits of voluntarily handing over more data than specifically required have probably disappeared with the UK GDPR's tougher data regulation regime. Among other things, the UK GDPR requires organisations to be transparent and provide information to individuals, to minimise use of personal data, to establish a legal basis for processing personal data and to legitimise any transfers of data outside the United Kingdom (and the EEA, under the GDPR). These obligations apply equally in data disclosures to authorities.

In relation to establishing a relevant legal basis for data processing, as well as the grounds discussed above (consent, legitimate interests, etc.), the 'legal obligation' basis may be relevant in responding to information requests and investigations by authorities. The UK GDPR and DPA 2018 provide that personal data may be disclosed to comply with a legal obligation (excluding contractual obligations), but only to the extent necessary to comply with that legal obligation: a proportionality test applies. This ground can only be relied on to justify data processing where a clear and binding legal obligation is present, under UK law. Obligations originating from outside the United Kingdom provide no legal basis for data processing on this ground, even where those obligations may be binding on a non-UK entity within an organisation's global corporate group, for example. Organisations should carefully document the relevant legal obligation, and the associated assessment of necessity and proportionality, to evidence UK GDPR compliance.

In international investigations, companies will need to address the GDPR restrictions and requirements for the transfer of personal data outside the United Kingdom or EEA. The considerations for organisations disclosing data to third-party authorities are slightly different from those concerning internal investigations. For example, reliance on individual consent or the SCCs is unlikely to be practicable. Transfers necessary to establish or defend a legal claim may be a helpful relevant ground in this context, though it is only available for occasional transfers, so may not be appropriate in ongoing investigations or longer-term engagement with authorities. An alternative basis to consider is provided by the EU GDPR and UK GDPR regime requirements for transferring data under international agreements, such as mutual legal assistance treaties (MLATs).[43] Using MLATs provides a structured system for exchanging information and evidence, but the process can be expensive and lengthy, which is particularly unhelpful where credit for early and responsive co-operation is sought, particularly when dealing with US authorities. The 2019 UK–US Bilateral Data Access Agreement aims to alleviate these

43 EU GDPR, Article 48; the UK GDPR does not mirror this specific provision, but the United Kingdom does recognise certain treaties on mutual legal assistance.

© Law Business Research 2021

concerns by providing a streamlined alternative to the MLAT process, though it is limited in scope to certain communications data held by communications services providers.[44]

As a general position, companies should be cautious when transferring data, even in response to requests from authorities.

Some national regulators (such as the Financial Conduct Authority and the US Securities and Exchange Commission) have reciprocal arrangements in place to transfer data. The use of these inter-regulator arrangements has a number of attractions. However, they often operate through a memorandum of understanding between the regulators, which on its face does not satisfy the definition of a legal agreement under Article 48 of the UK GDPR and so may not be an appropriate method for data transfer. While the interpretation of Article 48 of the UK GDPR remains untested, caution should be taken about permitting data to be transferred outside the jurisdiction under a memorandum of understanding between regulators.

See Chapters 11 and 12 on production of information to authorities

An alternative method for complying with the UK GDPR may be to redact personal information before handing documents over to authorities, depending on the size of the document set. This may, however, be a very expensive way of satisfying the authorities and the UK GDPR, particularly as it would require not only the data subject's name to be redacted, but also any information from which the data subject could be identified. Further, determining the appropriate approach to redaction is not always straightforward: data should be sufficiently redacted to satisfy the UK GDPR, but undue redaction may not be welcomed by the receiving authorities.

40.5 Investigations by authorities: US perspective

As in the United Kingdom, companies in the United States must be mindful of GDPR restrictions in responding to subpoenas or other compulsory demands requiring the production of documents. Under US law, a company served with compulsory demands must produce any responsive documents within its possession, custody or control – wherever the data is stored. To the extent that responsive data is stored in the European Union, and contains personal data subject to the UK GDPR or EU GDPR, the company must produce it notwithstanding its foreign location. As a result, US companies served with formal demands to produce documents may face a situation where their obligations to comply with US legal process conflict with the GDPR restrictions.

44 The UK–US Bilateral Data Access Agreement (signed on 3 October 2019) allows both US and UK law enforcement authorities to ask respective domestic courts to issue electronic data production orders directly against communications services provides in the other country, without going through the MLAT process. The text can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

© Law Business Research 2021

A US company concerned that it faces a conflict should first discuss the issue with the regulator or law enforcement agency involved and attempt to narrow the scope of the request to avoid or minimise the need to produce data regulated under UK GDPR or EU GDPR. This is particularly important because, for the company to rely on the legal defence derogation to produce the data to US authorities, the data must be '*necessary* for the establishment, exercise or defence of legal claims'.[45]

At the same time, US law enforcement authorities or regulatory agencies are likely to put the burden on the US company to show that the GDPR prevents the transfer and requires the company to identify all available bases to produce the documents.[46] Although the risk of breaching GDPR obligations should be a major consideration when dealing with investigating authorities, companies must balance this against the risks of non-compliance with US authorities, which may seek sanctions (including even criminal contempt) against a company for failing to comply with investigators' demands.

Where a company truly cannot comply with a demand for documents from US authorities without violating the transfer restrictions, and the company is unable to negotiate an adequate resolution with the US authorities, the company may choose to challenge the legal process. US courts have long held that, where it would violate foreign law for a company to produce certain documents in response to US legal process, the company may challenge enforcement based on international comity.

However, while courts have sometimes quashed subpoenas on comity grounds in civil litigation,[47] they have typically rebuffed such challenges of criminal investigations, finding that the domestic interest in enforcing the criminal laws trumped the foreign data privacy interests.[48] On the other hand, the prospect of significant GDPR penalties may lead US courts to give more weight to foreign data privacy interests than they might otherwise. Indeed, US court decisions applying the international comity balancing test have

45 UK GDPR, Article 49 / EU GDPR, Article 49 (emphasis added).

46 https://www.justice.gov/archives/opa/blog-entry/file/838386/download (US Department of Justice asserting that '[w]here a company claims that disclosure is prohibited, the burden is on the company to establish the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents').

47 See, e.g., *In re Cathode Ray Tube (CRT) Antitrust Litig.*, 2014 WL 1247770 (N.D. Cal. Mar. 26, 2014); *Motorola Credit Corp. v. Uzan*, 293 F.R.D. 595 (S.D.N.Y. 2013); *Tiffany (NJ) LLC v. Forbse*, 2012 WL 1918866 (S.D.N.Y. 23 May 2012).

48 See, e.g., *United States v. Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985) (according deference to judgment of Executive Branch that interest in enforcing criminal laws outweighed interest of Cayman Islands in preserving privacy of its banking customers); *In re Grand Jury Proceedings*, 532 F.2d 404 (5th Cir.), cert. denied, 429 U.S. 940 (upholding a grand jury subpoena against comity challenge based on foreign banking privacy laws).

© Law Business Research 2021

sometimes turned, in significant part, on the low likelihood of severe penalties being imposed by foreign authorities.[49]

40.6 Whistleblowers

The interplay between the increased protections for individuals under the UK GDPR and the protections for whistleblowers under existing laws is particularly interesting for practitioners and companies. More and more, internal and government investigations are triggered by information from (often anonymous) whistleblowers. Senior managers must be acutely aware of the respect to be shown to whistleblowers and whistleblowing laws, in particular with regard to anonymity and protection of the individual. The protection for whistleblowers is set to be strengthened across Europe, with the requirement on national legislatures to implement the EU Directive on whistleblowing protections by 17 December 2021.

40.6.1 Whistleblowing policies and data protection

Companies should have in place whistleblowing policies that respect the data protection principles – including specific whistleblower anonymity and privacy protections applicable in some jurisdictions – while also providing safeguards for the subject of the whistleblowing report, the whistleblower and third parties mentioned in the report. Companies must also ensure that by default, only personal data necessary for the specific purpose of investigating a whistleblowing report is processed.

40.6.2 Right to access

Where an individual's personal data has been processed during an investigation following a whistleblower report, the individual will still have the rights to access certain information as they would have done in any other circumstances. This includes the purpose and period envisaged for processing and how the data will be stored.[50] The personal information in a whistleblowing report can relate to whistleblowers, the persons under investigation, witnesses or other individuals mentioned, meaning that companies will need to uphold the data protection rights of all involved.[51]

---

49 Compare, e.g., *First City Nat'l City Bank*, 396 F.2d at 905 (compelling production of records notwithstanding potential conflict with German law, based in part on finding that the 'risk of civil damages [being imposed under German law] was slight and speculative') with, *Tiffany (NJ) LLC v. Qi Andrew, et al.*, 276 F.R.D. 143, 159 (S.D.N.Y. 2011) (declining to compel production given conflict with Chinese banking statute, where history of prosecutions demonstrated that the 'statute has been used to prosecute individuals and that violations can result in serious punishment').

50 UK GDPR, Article 15.

51 European Data Protection Supervisor: 'Whistleblowing' available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

© Law Business Research 2021

In addition, under the UK GDPR, employees may demand any personal data held about them by their employer. This, the European Data Protection Supervisor has noted, is 'of particular concern in the whistleblowing context as it could, theoretically, risk exposing a whistleblower's identity'.[52] The Article 29 Working Party[53] stated that the right to access data may be restricted to ensure the whistleblower's rights are protected and '[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement'.[54] This is reflected in the DPA 2018, which states that companies need not comply with a request for access to personal data if it would mean disclosing information about another individual who can be identified from that information, except if the individual has consented to the disclosure, or it is reasonable to comply with the request without that individual's consent.[55] Therefore, companies may be able to limit access to data following a whistleblower report, but they will still need to balance the data subject's right of access to personal data against the whistleblower's rights and the rights of any third parties mentioned in the report.[56]

See Chapters 19 to 21 on whistleblowers

Collecting, storing and accessing data: practical considerations 40.7

A few practical considerations for all investigations:

- Involve data controllers and other relevant organisations at as early a stage as possible.
- Identify any relevant documents to be transferred that contain special category data or any criminal offences data, and document the specific derogations or conditions on which that data will be used.
- Document all decision-making relating to the handling of that data (particularly any assessment of legitimate interests as a lawful basis for processing).
- Work with authorities to agree realistic expectations for the scope and timing of data requests.
- Consider all options for the transfer of data outside the United Kingdom or the European Union, including domestic review, redactions, MLATs and the use of domestic authorities, as well as the legal bases for transfer under GDPR; and document all decision-making relating to the international transfer of data.

52 ibid.

53 Now replaced by the EDPB.

54 Article 29 Data Protection Working Party, Opinion 1/2006, WP117 adopted 1 February 2006, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

55 DPA 2018, s.45.

56 European Data Protection Supervisor: 'Whistleblowing', available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

© Law Business Research 2021

41

Cybersecurity

Francesca Titus, Andrew Thornton-Dibb, Rodger Heaton, Mehboob Dossa and William Boddy[1]

41.1 Introduction

Cybercrime is a global threat that is constantly increasing in both volume and complexity. Perpetrators are using new technologies to commit cyberattacks against governments, corporates, critical infrastructure and individuals. The UK Government Cyber Security Breaches Survey 2021 showed that 39 per cent of businesses reported a cybersecurity breach or attack over the most recent 12-month survey period. This is higher among medium (65 per cent) and large (64 per cent) businesses.[2]

To tackle ever-increasing levels of cybercrime, countries around the world are introducing new laws focused on cybersecurity and data protection. Armed with new legal frameworks, regulators and law enforcement are placing onerous obligations on organisations who fall victim to cybercrime. There are shorter deadlines in which to notify the authorities of data breaches and ever increasing fines and penalties for businesses that fail to respond swiftly and appropriately to a cyberattack.

This chapter examines the complex area of cybersecurity and considers recent cases, the particular issues that can arise in cyber investigations and how to respond to a cyberattack. It identifies key considerations for corporates and their advisers in this ever-evolving area.

---

1 Francesca Titus, Rodger Heaton, Mehboob Dossa and William Boddy are partners, and Andrew Thornton-Dibb is an international attorney, at McGuireWoods.

2 UK Government Cyber Security Breaches Survey 2021, published 24 March 2021, available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

© Law Business Research 2021

What is cybercrime? 41.1.1

In the United Kingdom, cybercrime is an umbrella term used to define linked, but distinct, areas of criminal activity. Her Majesty's Government's National Cyber Security Strategy[3] defines these two subcategories as:

- cyber-dependent crimes – crimes that can only be committed through the use of information and communication technology (ICT) devices, where the devices are both the tool for committing the crime and the target of the crime; and
- cyber-enabled crimes – traditional crimes that can be increased in scale or reach by the use of computers, computer networks or other forms of ICT such as cyber-enabled fraud and data theft.[4]

In the United States, there is no uniform definition of cybercrime or cybersecurity, and the principal federal criminal law, the Computer Fraud and Abuse Act (CFAA), criminalises 'unauthorised access of computer systems'.[5] The Department of Justice's (DOJ) own manual on Prosecuting Computer Crimes sets out that '[its] focus is on those crimes that use or target computer networks, which [the DOJ] interchangeably refer[s] to as 'computer crime', 'cybercrime', and 'network crime'. Examples of computer crime include computer intrusions, denial of service attacks, viruses, and worms'.[6] The CFAA establishes the specific cybersecurity crimes of obtaining national security information, accessing a computer and obtaining information, trespassing in a government computer, accessing a computer to defraud and obtain value, intentionally damaging by knowing transmission, recklessly damaging by intentional access, negligently causing damage and loss by intentional access, trafficking in passwords, and extortion involving computers.

Globally cybercrime is a constantly evolving area, with perpetrators adapting their methods as new technologies become available. Several common types and techniques of cybercrime are as follows:

- Hacking is the targeted intrusion of a network, computer, mobile telephone, tablet or other electronic device.
- Malware is malicious software that interferes with computer operations and spreads across networks. Malware may be destructive, causing systems to crash or deleting files. It can also be used to steal data. Malware can be further sub-divided:
  - Viruses are software programmes loaded onto a user's computer covertly that perform malicious actions.

3 Her Majesty's Government National Cyber Security Strategy 2016–2021.

4 As defined in Her Majesty's Government National Cyber Security Strategy 2016–2021, p. 17.

5 18 USC § 1030.

6 Prosecuting Computer Crimes, Computer Crime and Intellectual Property Section Criminal Division, published by Office of Legal Education Executive Office for United States Attorneys.

© Law Business Research 2021

    - Trojans are malicious computer programmes that present themselves as useful, routine or interesting to persuade the victim to install them. The Trojan programme can then steal data or undertake other nefarious tasks under the guise of being the legitimate programme.
    - Spyware is software that gathers information from infected systems and monitors information such as key strokes or websites visited by a computer user. Spyware can be used to steal passwords, or financial or other valuable information.
    - Ransomware is software designed to block access to a computer system until a ransom is paid.
    - Worms are self-replicating programmes that spread from computer to computer causing damage. They do not require human interaction and do not need to attach themselves to software programmes.
- Phishing is the fraudulent practice of sending emails purporting to be from a reputable source to induce individuals to reveal personal information such as passwords or banking information.
- Fraudulent websites are increasingly common, they appear to be for legitimate businesses and trick victims into handing over financial information or payments.
- Denial of service (DoS) is a cyberattack in which the perpetrator disrupts a computer or other device to make it unavailable to users by disrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until it can no longer process normal users.
- A distributed denial of service (DDoS) attack is the same as a DoS but targets multiple network resources at once.

New technologies bring fresh opportunities for cybercriminals and there is already concern as to how artificial intelligence and 5G will be exploited by malicious actors.

41.1.2 Motivations of cybercriminals

Financial gain remains a key motivator for malicious cyber actors. Whilst some attacks are focused on the direct extraction of money, others seek to steal valuable information and either extract a ransom from the victim or sell the information to a third party.

While many cyberattacks are aimed at obtaining personal data through theft, other information such as trade secrets, compromising information, or information harmful to reputation can be valuable.

Increasingly, cyberattacks are being used for political and ideological reasons or to spread disinformation. Attacks can be a form of protest, and in these cases they usually focus on damage to infrastructure or control systems.

© Law Business Research 2021

Recent cyberattacks 41.1.3

Cyberattacks make headlines across the world, causing enormous reputational damage for the entities involved. Enforcement action frequently follows data breaches with ever increasing financial penalties for corporates. Many regulators also bring criminal enforcement action.

In summer 2021, Amazon's financial filings revealed that the Luxembourg data protection supervisory authority, the Commission Nationale pour la Protection des Données (CNPD), is fining the retailer's European arm (Amazon Europe Core Sàrl) €746 million for breaches of the EU's General Data Protection Regulation (GDPR).[7] The CNPD's decision is not yet publicly available so little is known about the facts, and it may not relate to a cyber incident. It is nevertheless worth mentioning as it is the largest GDPR fine on record and indicative of the enormous financial repercussions of not complying with data laws. Amazon has stated it intends to defend itself vigorously in the matter.

The year 2020 ended and 2021 began with the SolarWinds' Orion software breach, which impacted multiple US government agencies, including the US Treasury Department. Then in April 2021, Facebook confirmed that the personal information of more than 530 million users has been leaked and published on a hacking forum and is now subject to an investigation by the Irish Data Protection Commission. Most significant in terms of pure tangible impact was a ransomware attack on Georgia-based Colonial Pipeline that reportedly arose from a single compromised password, which effectively closed the supply of a key oil pipeline stretching from Texas to the Northeast of the United States, responsible for delivering 45 per cent of the East Coast's fuel. Colonial paid the hackers, an affiliate of a Russia-linked cybercrime group DarkSide, a US$4.4 million ransom shortly after the hack. In June 2021, the US Department of Justice announced that it had traced and seized US$2.3 million of cryptocurrency, being a portion of the total ransom paid by Colonial.[8]

Travelex, the world's largest retail currency dealer, received prominent media coverage in January 2020 after it suffered a ransomware attack.[9] Media reports attributed the hack to a cybergang called Sodinokibi, also known as Revil. Share value in Finablr, the parent company of Travelex, dropped in the week that followed the attack.[10]

Following an extensive investigation, the Information Commissioner's Office (ICO), which regulates data privacy in England and Wales, issued a

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)).

8 https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

9 National Cyber Security Centre Weekly Threat Report, 10 January 2020.

10 Caroline Binham and Kate Beioley, 'Travelex hackers demand ransom to protect data', *Financial Times* (8 Jan. 2020).

© Law Business Research 2021

notice of its intention to fine British Airways £183.39 million for infringements of data protection laws. The proposed fine related to a cyber incident notified to the ICO by British Airways in September 2018. The incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through the false site, customer details were being harvested by the attackers. Personal data of approximately 500,000 customers was compromised in the incident. British Airways was given the opportunity to make representations as to the level of financial penalty. In the end the ICO fined British Airways £20 million for failing to protect the personal and financial details of a number of its customers.[11]

Equifax is a multinational data, analytics and technology company with an emphasis on consumer credit reporting. In early September 2017, the US parent company announced it had been the victim of a criminal cyberattack. Although UK systems were not breached, the attack compromised personal information about some UK consumers.[12] The data breach exposed the personal information of 147 million people. The company agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau and 50 US states and territories. The settlement included up to US$425 million to help people affected by the data breach.[13]

The WannaCry cyberattack began on 12 May 2017 and, within a day, was reported by Europol to have infected more than 230,000 computers in at least 150 countries. This global attack quickly became a matter of public concern, with the UK's national media paying particular attention to the impact and the response of the National Health Service in England.[14] WannaCry was a ransomware, which targeted computers using the Microsoft Windows operating system. It infected computers by encrypting files on the computer's hard drive, making them impossible for users to access until a ransom had been paid in bitcoin to decrypt them. Both the United Kingdom and United States attributed the cyberattack to the North Korean Lazarus Group. Foreign Office Minister for Cyber, Lord Ahmad of Wimbledon, said: 'The UK's National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign – one of the most significant to hit the UK in terms of scale and disruption.'[15] The accusation had first been made by Thomas Bossert, an aide to President Donald Trump, in an interview with *The Wall Street Journal*.[16]

---

11 Information Commissioner's Office, press release, 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers' (16 Oct. 2020).

12 Cybersecurity incident – information for UK customers on Equifax website https://www.equifax.co.uk/incident.

13 Data breach settlement statement issued by Federal Trade Commission, January 2020.

14 Lessons learned review of the WannaCry Ransomware Cyber Attack, William Smart, Chief Information Officer for Health and Social Care, Independent Report (1 Feb. 2018).

15 UK Government Press Release published 19 December 2017.

16 'It's Official: North Korea Is Behind WannaCry,' *The Wall Street Journal* (18 Dec. 2017).

© Law Business Research 2021

In 2017 Yahoo!, the American web services provider, said that all three billion of its user accounts were affected by a hacking attack dating back to 2013. Yahoo! said that the data stolen during the attack did not include payment card or bank account data. The ICO eventually fined Yahoo! UK Services Limited £250,000 for the incident, which after investigation was said to have affected the personal data of approximately 500 million users worldwide.[17]

Uber Technologies Inc was caught in a data controversy when it was reported that hackers stole the personal data of 57 million customers and drivers. Compromised data from the October 2016 attack included names, email addresses and phone numbers, the company reported. It was reported that the breach took place in 2016 but that Uber sought to conceal the event. The company is said to have paid hackers US$100,000 to delete the data that had been taken from Uber's cloud-based servers.[18]

The ICO fined Uber £385,000 in what it called 'a series of avoidable data security flaws which allowed the details of around 2.7 million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers'.[19]

The ICO was strong in its criticism of the company's director of investigations, Steve Eckersley, saying:

> *This was not only a serious failure of data security on Uber's part, but a complete disregard for the customers and drivers whose personal information was stolen. At the time, no steps were taken to inform anyone affected by the breach, or to offer help and support. That left them vulnerable.*[20]

The financial penalties in the United States totalled US$148 million.[21] Lisa Madigan, the Illinois Attorney General, stated:

> *This is one of the most egregious cases we've ever seen in terms of notification; a yearlong delay is just inexcusable. And we're not going to put up with companies, Uber or any other company, completely ignoring our laws that require notification of data breaches.*[22]

17 Information Commissioner's Annual Report and Financial Statements 2018–2019, p. 25.

18 Thomas P Bossert, 'Uber pays $148 m over data breach cover up', BBC News (27 Sep. 2018).

19 Information Commissioner's Office, press release, 'ICO fines Uber £385,000 over data protection failings' (27 Nov. 2018).

20 Id.

21 *People of the State of Illinois v. Uber Technologies Inc.*, No. 2018-CH-000304, final judgment and consent decree, September 2018.

22 Associated Press, 'Uber agrees to $148M settlement over data breach' (26 Sep. 2018).

© Law Business Research 2021

41.2 Legal framework

41.2.1 United Kingdom

Within the United Kingdom, there are a number of different Acts and Regulations that may be applicable to a cyber incident, depending on the facts and the type of entity that has been targeted.

41.2.1.1 UK legislation criminalising cyberattacks

The Computer Misuse Act 1990 (CMA) is the key legislation in the United Kingdom relating to offences or attacks against computer systems. The CMA allows proceedings to be brought in England or Wales if, in the circumstances of the offending, there is at least one significant link with the United Kingdom.[23]

The CMA criminalises unauthorised access to computer material,[24] unauthorised access with intent to commit or facilitate commission of further offences,[25] and unauthorised acts with intent to impair the operation of a computer,[26] causing or creating risk of serious damage for example to the environment or economy.[27]

Under section 3(1) of the Investigatory Powers Act 2016, which came into force in June 2018, it is an offence to intentionally intercept a communication in the United Kingdom, without lawful authority, in the course of its transmission by means of a public or private telecommunication system or a public postal service.

Additionally, some offences under the Data Protection Act 2018[28] (DPA) such as knowingly or recklessly obtaining or disclosing personal data without consent, procuring the disclosure of personal data to another person without consent, and selling personal data disclosed or retained without consent, can be relevant to cybercrime.[29]

Many types of crime, of course, do not depend on computers or networks but are being committed with relative ease using the internet. These offences include fraud, intellectual property crime and sending malicious communications, which are dealt with under separate legislation.

23 Computer Misuse Act 1990, s.4.

24 ibid., s.1.

25 ibid., s.2.

26 ibid., s.3.

27 ibid., s.3ZA; this section is aimed at attacks on critical national security.

28 The Data Protection Act 2018 (DPA) updated and replaced the Data Protection Act 1998 when it came into force on 25 May 2018. It was thought that the older Act did not adequately provide for the modern digital age.

29 DPA, ss.170 to 173.

© Law Business Research 2021

UK laws leading to positive obligations for victims of cyberattacks 41.2.1.2

The United Kingdom has a robust set of laws relating to data breaches that commonly arise out of cyberattacks. The EU GDPR has been incorporated directly into UK law as the UK GDPR.[30]

Article 5 of the UK GDPR sets out the key principles, rights and obligations for most processing of personal data, but it does not apply to processing for law enforcement purposes. The seven key principles are (1) lawfulness, fairness and transparency (2) purpose limitation, (3) data minimisation, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality, (7) accountability.

The UK GDPR is concerned with 'personal data', which means information about a particular identified or identifiable living individual; it includes employees, clients, business contacts, public officials and members of the public. If it is possible to identify someone from the details, or by combining the details with other information, then it will still come within the scope of what is 'personal data'. What identifies an individual includes names, numbers, cookie identifiers and internet protocol (IP) addresses.

The law is designed to be flexible and to take a risk-based approach to data protection. In reality, the legislation puts the onus on organisations to think about, and if necessary be able to justify, how they use data and process data.

The UK GDPR applies to the processing of 'personal data' if that is completed wholly or partly by automated means or the processing other than by automated means of personal data that forms part of, or is intended to form part of, a filing system. Processing includes collecting, recording, storing, using, analysing, combining, disclosing or deleting data. For the majority of organisations handling data, the processing test will easily be met.

Organisations processing 'personal data' need to ensure they have appropriate security measures in place to protect the data held. This is the integrity and confidentiality principle (or security principle) of the UK GDPR. Under this principle, organisations must have appropriate technical and organisational measures in place. This may be achieved via risk analysis, organisational policies, and physical and technical actions. The costs of implementation when deciding what measures to take are relevant, but must be appropriate to the circumstances of the organisation and the risk the processing poses.

The measures in place must enable custodians of 'personal data' to restore access and availability of 'personal data' in a timely manner in the event of a physical or cyber incident. There need to be processes in place to test the effectiveness of measures, and where improvements are required these should be implemented.

30 The UK GDPR is the retained EU law version of the GDPR as it forms part of the law of England, Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018, s.3, as amended by Schedule 1 to the Date Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 SI 2019/419.

© Law Business Research 2021

The UK GDPR does not define the security measures an organisation needs to have in place, but some industries are required to meet certain standards by their regulator or industry body; for example the Financial Conduct Authority Handbook covers Data Security in Financial Services, which includes the risk that customer data is lost or stolen.[31] Whether such requirements have been adhered to is likely to be relevant to enforcement action.

The DPA sets out the data protection framework in the United Kingdom alongside the UK GDPR. It contains three separate data protection regimes: part 2 sets out a general processing regime (the UK GDPR); part 3 sets out a separate regime for law enforcement authorities; and part 4 sets out a separate regime for the three intelligence services. The DPA was amended on 1st January 2021 to reflect the United Kingdom leaving the European Union.

Other laws relevant to privacy in which obligations for corporates can be found are the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR),[32] which is concerned with electronic communications and specific rules for emails, texts, cookies, location data and itemised billing. PECR is predominantly concerned with public electronic communications networks or services, but it applies to organisations that use cookies or similar technology on their website, or market by telephone, email, text or fax. Following Brexit, the UK GDPR sits alongside PECR with some overlap.

The Network and Information Systems Regulations 2018 (NIS)[33] are intended to combat the threats posed to network and information systems with a desire to improve the digital economy and society. NIS applies to operators of essential services and relevant digital service providers such as online search engines, online marketplaces and cloud computing services.

Numerous other Acts of Parliament can be relevant to data breaches. The facts of any particular case will determine which apply. The Acts can be as diverse as the Official Secrets Act 1989, dealing with information that can impact national security,[34] and the Companies Act 2006, imposing duties on directors to adhere to a desirability a company maintain a reputation for high standards.[35] It is advisable to engage external counsel for specialist legal advice if dealing with a data breach.

41.2.2 United States

The United States has a medley of unrelated, and at times incompatible, federal and state laws and regulatory guidance, which either relate specifically to cybersecurity or have been interpreted to do so, and no uniform national law that

31 The Financial Conduct Authority Handbook.

32 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

33 The Network and Information Systems Regulations 2018.

34 Official Secrets Act 1989, s.1.

35 Companies Act 2006, s.172(1)(e).

© Law Business Research 2021

explicitly requires security of personal information across all industries and sectors. This results in there being no generally accepted approach to defining 'cybersecurity' and no nationally recognised manner in which companies can maintain systems and procedures to adequately address cybersecurity risks. The diversity of laws and the rapidly evolving regulatory environment mean there are a number of potential public and private litigants and that businesses operating across the United States need to carefully assess their cybersecurity risks and compliance requirements. In 2020, at the state level alone, 38 states introduced or considered more than 280 bills or resolutions significantly related to cybersecurity, and 20 states enacted cybersecurity-related bills.[36] It is advisable to seek the assistance of external counsel when dealing with this specialised area of law.

Federal law 41.2.2.1

The CFAA

The CFAA provides for numerous cybersecurity-specific offences relating to unauthorised access of computer systems and related damage, trafficking and extortion. Notably, the US Supreme Court recently narrowed the scope of liability under the CFAA, holding that it only covers information obtained for an improper purpose if the person accessing the information was unauthorised to access it.[37]

The FTC and the Federal Trade Commission Act

The Federal Trade Commission (FTC) is a federal agency tasked with protecting consumers and promoting competition in the United States through the enforcement of civil antitrust and consumer protections laws. The FTC has powers pursuant to the Federal Trade Commission Act (FTCA),[38] which prohibits 'unfair or deceptive acts or practices in or affecting commerce', regardless of industry.

Financial institutions and the Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), enforced by multiple federal agencies, requires financial institutions to maintain safeguards for non-public information in the institutions' control and to adopt 'administrative, technical, and physical safeguards' for the security of 'non-public personal information'.[39] In sum, the GLBA requires that financial institutions have policies and procedures reasonably designed to ensure the security and confidentiality of customer's records and to protect against cybersecurity threats and unauthorised access and uses of customer records.

36 National Conference of State Legislatures, at https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx.

37 V*an Buren v. United States*, 141 U.S. 1648 (2021).

38 15 U.S.C. § 45(a)(1) (2012).

39 The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2018).

© Law Business Research 2021

Various agencies have published guidelines pursuant to the GLBA, including the 'Interagency Guidelines' adopted by the Office of the Comptroller of the Currency, the Federal Reserve System and the Federal Deposit Insurance Corporation.[40] The guidelines prescribe steps for institutions including involving the board in the development of a cybersecurity programme, conducting risk assessments, and conducting due diligence and ongoing monitoring of service providers' cybersecurity measures.

Publicly traded companies

The Securities and Exchange Commission (SEC) has published guidance on publicly traded companies' disclosure obligations with respect to cybersecurity and on companies disclosing material cybersecurity risks and incidents to investors.[41] This guidance recommends that publicly traded companies adopt controls and procedures that enable companies to identify cybersecurity risks and incidents, assess and analyse their impact on a company's business, evaluate their significance and make timely disclosures. The guidance also recommends that companies implement measures to prevent insider trading in the event of and during the investigation of a potential data breach.

Healthcare providers and the Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA)[42] requires that healthcare providers, health plans, healthcare clearing houses, (and in certain cases business associates) adopt 'administrative, technical, and physical safeguards' to protect individually identifiable health information (protected health information or PHI). HIPAA restricts access to and use of PHI while imposing related security standards (the Security Rule), and a requirement to notify individuals affected by any breach of privacy (the Breach Notification Rule). Finally, HIPAA provides for civil and criminal penalties for the compromise of PHI maintained by entities covered by the statute (covered entities) and business associates.

The Federal Information Security Management Act

The Federal Information Security Management Act (FISMA)[43] defines a framework for managing information security that must be followed by all information

40 Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. § 208 app. D–2 (2016).

41 SEC Statement and Guidance on Public Cybersecurity Disclosures, 17 C.F.R. §§ 229, 249 (2018).

42 Health Insurance Portability and Accountability Act of 1996 § 1173, 42 U.S.C. § 1320d2(d)(2) (2012); see also 45 C.F.R. §§ 164.302–164.318 (2016) (outlining the Department of Health and Human Services' security-standard regulations authorised by HIPAA).

43 44 U.S.C. §§ 3541–3549 (2012).

© Law Business Research 2021

systems used or operated by a US federal government agency and by third-party contractors who work on behalf of a federal agency in those branches. Failure by a contractor to comply with FISMA can result in loss of federal funding.

The Cybersecurity and Infrastructure Security Agency Act

The Cybersecurity and Infrastructure Security Agency Act (CISAA)[44] enables private entities to monitor information systems for cybersecurity purposes; operate 'defensive measures' for cybersecurity purposes;[45] and most notably to share information about cyber-threat indicators or defensive measures with other private entities or the federal government,[46] provided that private entities take steps to remove personal information before sharing any such cyber-threat indicators.[47]

State law 41.2.2.2

At least 25 states have laws that address data security practices of private sector entities, the majority of which require companies to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorised access, destruction, use, modification or disclosure.[48] As examples:

- New York requires that companies develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information including, but not limited to, disposal of data;[49]
- California requires companies to implement and maintain reasonable security procedures and practices appropriate to the nature of the information; and[50]
- Massachusetts requires companies to take specific steps to assess security risks, train employees, oversee service providers and implement other safeguards.[51]

---

44 6 U.S.C. § 1503(a)(1) (2012).

45 Id. § 1503(b). The statute defines 'defensive measure' as 'an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability,' and explicitly excludes any 'measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system' and is not owned by the entity operating the defensive measure or another entity that has provided consent. Id. § 1501(7)(A)–(B).

46 Id. § 1503(c)(1).

47 Id. § 1503(d)(1)–(2).

48 See National Conference of State Legislatures, Data Security Laws Private Secto,r available at https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#Overview.

49 New York Gen. Bus. Law § 899-BB.

50 Cal Civ. Code § 1798.81.5.

51 201 Mass. Code Regs. 17.03 (2009).

© Law Business Research 2021

All 50 states, the District of Columbia and other US jurisdictions have imposed data breach notification requirements on private entities that collect or process personal data, which can require notice to consumers, regulators, law enforcement or credit bureaus.[52] Some states only require notice if the business determines that there is a reasonable likelihood of harm,[53] while others require notification regardless of the determination of likelihood of harm.[54] The requirements also may conflict. For example, Massachusetts prohibits any description of how a data breach occurred,[55] while other states require a brief description of the incident.[56] Notably, some state notification laws establish jurisdiction based on whether the data subject is located in the state and so can apply to a company regardless of where it is located.[57]

41.3 Proactive cybersecurity

Mr Ciaran Martin, the former head of the United Kingdom's National Cyber Security Centre stated in 2020: 'Every organisation now knows they need to understand cybersecurity risk just as they need to understand financial, legal risk and so on.'[58] It is now a key function of business to have a comprehensive cybersecurity programme in place.

The UK GDPR specifically requires organisations to have a process for regular testing, assessing and evaluating of the effectiveness of any information security measures put in place. However, the type of tests and how regularly they are carried out is for the organisation to assess in light of its particular circumstances.

Policies should be in place that are regularly reviewed (many organisations now review their policies every quarter, such is the pace of change in this area) and updated as part of a regular cybersecurity audit. Depending on the characteristics of the business, third parties, such as businesses in its supply chain, may need to form part of the audit and assessment process. It is common for cybercriminals to breach networks via trusted business partners.

---

52 For a list of all data breach notice statutes, see Security Breach Notification Laws, Nat'l Conf. St. Legislatures (12 Apr. 2017), at http://www.ncsl.org/research/telecommunicationsand-information-technology/security-breach-notification-laws.aspx.

53 See, e.g., Mich. Comp. Laws Ann. § 445.72 (West 2019) (requiring notice unless the organisation determines that 'the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state[.]').

54 See, e.g., Cal. Civ. Code § 1798.82 (West 2019).

55 Mass. Ann. Laws ch. 93H (LexisNexis 2019).

56 See, e.g., Iowa Code § 715C.2 (2019) (requiring data breach notices to include a 'description of the breach of security.').

57 See, e.g., Iowa Code § 715C.2 (2019) ('Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security.').

58 Peter Foster, 'Cyber chief warns of east-west split over the internet', *Financial Times* (Aug. 2020).

© Law Business Research 2021

Good cybersecurity relies on education and awareness. Regular training of staff is key and should include temporary and contract staff.

Physical security, concerning access to premises and equipment, also needs to be addressed. All organisations need to consider storage arrangements and secure disposal of records that are no longer required.

Computer and network security will in most cases require technical expertise. During the covid-19 pandemic, remote working raised new risks which all organisations should have been conscious of and working to reduce. Of particular concern are removable media and vulnerabilities of multiple internet connections.

There need to be protocols to cover password use, firewalls, regular updates for software, backup and restoration of electronic information and monitoring to detect breaches.

Organisations should have a cyber-breach response plan to assist in the detection of cybercrime and ensure incidents are responded to swiftly, efficiently and comprehensively. There should be a clear structure of responsibility to allow for accountability.

Conducting an effective investigation into a cyber breach 41.4

The aim of an investigation will be to understand the scope and impact of the cybersecurity incident. The findings of the investigation will be put to multiple uses, including preventing repetition of the incident, managing all the repercussions, helping with reputational damage, assisting with operational disruption, and identifying harm to clients. This will also be key to enforcement action, so it is vital that the investigation be properly conducted. It is advisable to engage external legal counsel as soon as a breach has been detected or is suspected. This is particularly important for the protection of legal professional privilege.

See Chapters 36 and 37 on privilege

The early stages of the investigation are likely to be critical and urgent. In Europe, the GDPR requires organisations to have robust breach detection and an investigation procedure in place. It is sensible to use the protocols that the organisation has in place with the benefit of legal advice. Records need to be kept of the breach and response regardless of whether the matter is ultimately reported to the authorities.

Digital evidence is likely to need to be gathered and care must be taken to establish a clear picture of what happened without compromising evidence. It may be necessary to engage third-party forensic experts. For privilege and continuity, this is best done through external legal counsel.

See Chapter 22 on forensic accounting

It is likely that there will be interviews with employees who may have contributed to the incident, for example, through downloading a malicious programme. Staff who first responded to the incident and those who may have had their personal data compromised may all need to be interviewed. It is likely to be too early to anticipate all the legal actions that may flow from the incident, so it is sensible to secure evidence in accordance with the law so it can be used as required, and if necessary at a trial. For example, in the United

See Chapters 7 and 8 on witness interviews

© Law Business Research 2021

States an *Upjohn* warning may be appropriate if interviewing staff.[59] Take local law advice from experienced cybersecurity counsel.

41.5 Enforcement

Dependent on where the cyberattack took place, where an organisation is located, where the data is held (which with the use of cloud technologies is now commonly multiple locations) and in some cases where the individuals whose data has been compromised are located, there are often several enforcement authorities with an interest in the event.

41.5.1 Enforcement in England and Wales

In most of the United Kingdom,[60] the ICO is the independent authority in charge of upholding information rights in the public interest. In addition to enforcement activities, the ICO offers guidance and seeks to promote good practice by carrying out audits and monitoring compliance and complaints.

41.5.2 Reporting a breach in England and Wales

In England and Wales there is a legal requirement that certain incidents must be reported to the ICO, and this has to be done within hours of the breach. For example, if there has been a 'personal data breach', this must be reported to the ICO. A personal data breach is a breach of security leading to 'the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. Such a breach must be reported within 72 hours of the organisation becoming aware of it, unless it can be demonstrated that it is unlikely to result in a risk to individuals' rights and freedoms.

If there is a high risk to individuals' rights and freedoms, the individuals concerned should be informed without delay.

See Chapter 3 on self-reporting to authorities

Corporates and their advisers should assume that information provided to one data regulator will be passed on to others and that this could give rise to liabilities in multiple jurisdictions. However, the organisation should ensure it meets its reporting obligations in all jurisdictions applicable to the incident.

41.5.3 Enforcement in the United States

As referenced above, a range of general and industry-specific federal and state regulators may investigate and bring enforcement actions related to cybersecurity incidents. While too numerous and detailed to discuss for the purposes of this chapter, the FTC (which has general jurisdiction over companies operating in the US), the SEC (which has jurisdiction over publicly traded

59 In an *Upjohn* warning, an employee is advised by company counsel that counsel is acting for the company, privilege in the interview is the company's and the company may waive that privilege in disclosing details of the interview to authorities or third parties. *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

60 Scotland has its own Information Commissioner.

© Law Business Research 2021

companies) and the DOJ are active in bringing enforcement actions in relation to cybersecurity incidents. Acting pursuant to the FTCA, which prohibits 'unfair or deceptive acts or practices in or affecting commerce', the FTC has brought cybersecurity related enforcement actions on the basis of both 'deceptive' and 'unfair' practices by companies, including for misrepresenting data security practices,[61] failure to properly safeguard personal data,[62] failure to use adequate encryption for medical records,[63] negligent supervision of service providers responsible for handling sensitive information,[64] failure to provide adequate cybersecurity training to employees,[65] failure to disclose privacy practices adequately[66] and using data absent informed consent.[67] The SEC has investigated and brought enforcement actions against public companies following cybersecurity incidents, including for companies' failure to appropriately disclose material cybersecurity risks contrary to the SEC's guidance. The DOJ investigates and prosecutes cybercrime activities pursuant to the CFAA, as illustrated on 8 June 2021 when the DOJ indicted the chief operating officer of an Atlanta-based network security company, for allegedly conducting a cyberattack on a medical centre in violation of the CFAA.[68]

The New York Department of Financial Services (DFS), which supervises and regulates the activities of insurance companies, banking and other financial institutions in the state of New York, has investigation and enforcement powers pursuant to the DFS Cybersecurity Regulation. This imposes strict cybersecurity rules on covered organisations and subjects them to the risk of financial penalty. In July 2020, three years after the DFS Cybersecurity Regulation's initial

61 See, e.g., Complaint at 3–5, *In re Upromise, Inc.*, FTC File No. 102-3116, No. C-4351 (F.T.C. 27 Mar. 2012), 2012 WL 1225058.

62 See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245 (3d Cir. 2015) ('A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.').

63 Complaint at 4, *In re Henry Schein Practice Sols., Inc.*, FTC File No. 142-3161, No. C-4575 (F.T.C. 20 May 2016), 2016 WL 160609.

64 Complaint at 3–4, *In re GMR Transcription Servs., Inc.*, FTC File No. 122-3095, No. C-4482 (F.T.C. 3 Feb. 2014), 2014 WL 492352.

65 Complaint at 2, *In re Franklin's Budget Car Sales, Inc.*, File No. 102-3094, No. C-4371 (F.T.C. 3 Oct. 2012), 2012 WL 5375157.

66 See, e.g., Complaint, *In re Sears Holdings Mgmt. Corp.*, Docket No. C-4264, para. 4 (F.T.C. 9 Sep. 2009). (The FTC brought an enforcement action in 2009 against Sears for allegedly failing to disclose adequately the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software).

67 Complaint, *In the Matter of Myspace LLC*, Docket No. C-4369 (F.T.C. 11 Sep. 2012).

68 US Dep't of Justice, Press Release, 'Chief Operating Officer of network security company charged with cyberattack on Gwinnett Medical Center' (10 Jun. 2021), available at https://www.justice.gov/usao-ndga/pr/chief-operating-officer-network-security-company-charged-cyberattack-gwinnett-medical.

© Law Business Research 2021

release, DFS announced its first enforcement action against First American Title Insurance Company seeking monetary penalties and injunctive relief for purported violations of six provisions of the DFS Cybersecurity Regulations. In March 2021, DFS announced its first penalty pursuant to a settlement with Residential Mortgage Services, Inc, which imposed a US$1.5 million penalty in relation to a 2019 data breach disclosed to DFS during a routine safety and soundness examination in 2020. In April 2021, DFS announced a US$3 million penalty pursuant to a settlement with National Securities Corporation in relation to four cyber breaches that occurred between 2018 and 2020 that exposed National Securities' customers sensitive and non-public personal data.

While not enforcement action *per se*, the threat of civil litigation (class actions in particular) by private parties for damages arising from cybersecurity incidents is very real. Cybersecurity-related civil claims have been brought on a variety of theories, including for negligence,[69] negligent misrepresentation,[70] unfair or deceptive trade practices pursuant to state consumer protection statutes,[71] breach of contract,[72] breach of implied warranty[73] and unjust enrichment.[74] A recent example of this followed the SolarWinds breach, where investors filed a class action suit on 1 April 2021 against SolarWinds alleging that it had made materially false and misleading statements to the market in connection with the software breach.[75]

41.5.4 Reporting a breach in the United States

A mass of general and industry specific federal and state laws require notification of cybersecurity incidents too numerous to discuss in detail for the purposes of this chapter. Given the range of possible notification requirements, it would be prudent for any company operating in the United States to map out all notification requirements applicable to its operations, and to identify processes for sharing of information with private and public entities pursuant to CISAA.

See Chapter 4 on self-reporting to authorities

69 See, e.g., *Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc.*, 892 F.3d 612, 616 (4th Cir. 2018), and *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014).

70 See, e.g., *In re Zappos.com, Inc.*, No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3–4 (D. Nev. 9 Sep. 2013).

71 See, e.g., *In re Yahoo! Customer Data Security Breach Litigation*, 313 F. Supp. 3d 1113, 1128 (N.D. Cal. 2018).

72 See, e.g., *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 970 (N.D. Cal. 2016).

73 See, e.g., *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 119–20 (D. Me. 2009), aff'd, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011).

74 See, e.g., *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014).

75 The first complaint, subsequently amended, was first filed on 9 February 2021. See Complaint, *In re SolarWinds Corporation Securities Litigation*, 1:21-cv-00138 (W.D. Tex. 2021) (No. 1).

© Law Business Research 2021

42

Directors' Duties: The UK Perspective

Nichola Peters, Michelle de Kluyver and Jaya Gupta[1]

Introduction 42.1

Corporate governance has become increasingly important in the context of financial crime compliance and investigations. One reason for the development is that good corporate governance is a foundation for asserting substantive legal defences to allegations of misconduct. Legislative developments such as the introduction of the UK Bribery Act 2010 and the Criminal Finances Act 2017 mean that the board's responsibilities for identification, mitigation and ongoing review of financial crime risk have a material impact on whether companies can defend allegations of criminal conduct by associated persons (those providing services to the company). The 'adequate procedures' and 'reasonable prevention procedures' defences contained in that legislation require companies to demonstrate 'top-level commitment' to managing financial crime risk and to show that they have understood and managed their financial crime risks proportionately by reference to the nature, scale and complexity of their operations. In the financial services sector, senior managers in firms subject to the Senior Managers and Certification Regime (SMCR) will have specific statements of responsibilities for which they can be held to account.

In 2014 the United Kingdom introduced deferred prosecution agreements (DPAs) as a new mechanism for resolving corporate criminal investigations where there is evidence of criminal conduct. DPAs have added to the focus on corporate governance. Factors that influence whether to offer a company a DPA resolution include whether the company has an effective compliance programme, the composition and conduct of the management team, and the extent to which corporate structures or processes have been changed to

See Chapter 23 on negotiating global settlements

1 Nichola Peters, Michelle de Kluyver and Jaya Gupta are partners at Addleshaw Goddard LLP.

© Law Business Research 2021

mitigate identified risks. A company's prevention procedures are therefore relevant to corporate outcomes even where they fall short of the legislative standard required to establish a substantive defence. A company's commitment to compliance will also be taken into account in calculating the level of fines or other penalties.

The issue of how companies manage themselves and identify and mitigate risks has therefore become central in financial crime investigations. Indeed, an investigations process forms part of a company's prevention procedures and companies should take care to ensure that investigations are sufficiently independent and appropriately robust. Where there are allegations of misconduct that may entail significant reputational or commercial risk, the board (or a board subcommittee) is likely to provide oversight of particular investigations, in addition to providing oversight of a company's overall compliance obligations. Directors can also be compelled to give evidence as witnesses in government investigations to explain (among other issues) their company's approach to compliance.[2]

In significant investigations, and subject to managing conflicts of interest, the board is likely to be involved in making strategically important decisions such as whether to self-report suspected misconduct and how to resolve findings of misconduct in a major investigation.

It is therefore important that directors are aware of the multiple sources of their duties and obligations and how they are likely to apply both to the board's oversight obligations regarding the management of financial crime risk and in individual investigation scenarios.

42.2 Sources of directors' duties and responsibilities under UK law

The core duties owed by directors to their companies are set out in sections 171 to 178 of the Companies Act 2006 (CA 2006). Directors may also have additional duties depending on the company they serve. The commentary below identifies and explains the key sources of governance obligations for directors in the United Kingdom. As a result of the global financial crisis and high-profile examples of corporate collapse, the legislative and regulatory framework is increasingly focused on integrity, accountability and driving high standards of business conduct. As part of the government's reform of audit and corporate governance, there are proposals to create a new set of regulatory duties for directors based on the CA 2006 and to introduce new ethics rules for directors that would be enforceable by the proposed Audit, Reporting and Governance Authority (ARGA, successor to the Financial Reporting Council (FRC)).

2 Directors can also become suspects in an investigation, of course, but this chapter focuses on oversight responsibilities and not directors' individual defence rights.

© Law Business Research 2021

Companies Act 2006 42.2.1

The duty to act within powers (section 171 CA 2006) 42.2.1.1

Directors are not permitted to abuse their powers.[3] They must act in accordance with the company's constitution, which includes its articles of associations, resolutions, decisions and investment agreements. In addition, directors are only permitted to exercise their powers for the purposes for which they are conferred, called the 'proper purpose test'. The question of whether a power has been exercised properly will turn on whether the 'substantial' or 'dominant' purpose for which it was exercised was the purpose for which it was conferred.[4] Directors must not exercise their powers to protect their own positions. If power is exercised for a wrongful purpose, the use to which that power is put is voidable.

In the context of a financial crime investigation, it would be an improper use of power if a director sought to prevent, control or influence an investigation to protect his or her own position. A director in this position would also have a conflict of interest, which would engage the separate duty to avoid conflicts of interest. The conduct would also likely breach the duty to promote the success of the company. Investigators must always be alive to the risk of conflicts of interest within the investigation team and in the reporting line.

Duty to promote the success of the company (section 172 CA 2006) 42.2.1.2

The duty to promote the success of the company is relevant to almost everything a director does. The duty requires directors to act in good faith in a way they consider would be most likely to promote the success of the company for the benefit of its members as a whole.[5] The courts will typically respect the decisions of the board provided that they reach the standard of a good-faith business judgment.

When discharging their duties to promote the success of the company, directors must have regard to a list of factors, including:

- the likely consequences of any decision in the long term;
- the interests of the company's employees;
- the need to foster the company's business relationships with suppliers, customers and others;
- the impact of the company's operations on the community and the environment;
- the desirability of the company maintaining a reputation for high standards of business conduct; and
- the need to act fairly as between members of the company.

3 Companies Act (CA) 2006, s.171.

4 *Howard Smith Ltd v. Ampol Petroleum Ltd* [1974] A.C. 821; *Eclairs Group Ltd v. JKX Oil & Gas Plc* [2015] UKSC 71; [2016] 3 All ER 641.

5 CA 2006, s.172.

© Law Business Research 2021

The list of factors is not exhaustive. Directors may balance the various factors and they must take into account any other factor that would be relevant to a particular decision.[6]

The Association of General Counsel and Company Secretaries of the FTSE 100 (GC100) and the Chartered Governance Institute (formerly The Institute of Chartered Secretaries and Administrators (ICSA)) have published useful, practical guidance notes relevant to the interpretation and application of this duty.[7] The GC100 Guidance on Directors' Duties, section 172 and Stakeholder Considerations (GC100 Guidance) states: 'The factors are designed to ensure that, in promoting the success of the company, broader implications of decisions are considered by the directors. You may find it helpful to see the duty as about creating a culture in the business, so that when you take decisions, their wider impact has been considered.'

The duty to promote the success of the company is intertwined with the duty to act with reasonable care, skill and diligence set out in section 174 of the CA 2006. The GC100 Guidance states: 'The section 172 duty must be fulfilled by a director in accordance with the duty of care, skill and diligence imposed by section 174.'

An interesting application of the duty to promote the success of the company to investigations is that where directors may be implicated in misconduct, they must disclose their own wrongdoing.[8] A director who asserts the privilege against self-incrimination will therefore breach this duty.

In insolvency situations, the interests of creditors will take precedence over the interests of members. This can materially change how the board approaches an investigation. A company's solvency position can change for reasons unrelated to the investigation but also for reasons central to the investigation, such as where there has been an internal fraud. If there are concerns about the company's solvency, directors should proactively seek legal and financial advice as to their altered duties. The duties owed under sections 171 to 177 of the CA 2006 do continue even after the relevant company has entered into an insolvency procedure.[9]

For periods beginning on or after 1 January 2019, most UK-incorporated companies are required to report on the company's performance of the duty under section 172 of the CA 2006.[10] The government believes that by imposing reporting obligations linked to this duty, directors will consider the wider stakeholder issues more carefully and that boardroom engagement will be

See Section 42.2.6

6 *Re Phoenix Contracts (Leicester) Ltd* [2010] EWHC 2375 (Ch).

7 The GC100 Guidance on Directors' Duties (2007); The GC100 Guidance on Directors' Duties: Section 172 and Stakeholder Considerations (2018); ICSA Guidance Note Directors' General Duties.

8 *Item Software (UK) Ltd v. Fassihi* [2004] EWCA Civ 1244.

9 As discussed in *Hunt (as Liquidator of System Building Services Group Ltd) v. Michie & Ors* [2020] EWHC 54 (Ch).

10 The Companies (Miscellaneous Reporting) Regulations 2018.

© Law Business Research 2021

improved. In 2018, the FRC published its Revised Guidance on the Strategic Report to assist companies in their reporting. The FRC's Financial Reporting Lab has also published a report on reporting on stakeholders, decisions and section 172, which outlines what investors want to see reported and provides examples of helpful ways of addressing these requirements.[11] It is believed that the enhanced reporting obligations for non-financial information will result in more trust and transparency in business, but this is an area that remains closely monitored by the FRC.

General oversight obligations and oversight of material investigations

The duty to promote the success of the company is central to the directors' obligations to ensure that a company identifies and mitigates its financial crime risks.

The GC100 Guidance recommends that directors ensure that they receive the information they need to carry out their roles and satisfy the duty. In the context of the board's oversight duties in relation to compliance, directors should satisfy themselves that both the quality and frequency of the management information they receive is adequate. Directors need to understand the company's risk profile and risk assessment, and how the compliance programme responds to these risks. In addition, directors should expect to receive periodic reporting to satisfy themselves that the procedures adopted remain fit for purpose. There is no one-size-fits-all approach, and the detail and frequency of management information will depend on the size, complexity and risk profile of the organisation. Data about non-material issues and investigations will often be aggregated and shared annually. Where the board has oversight of a material investigation, they are likely to require more detailed information and regular information flows. The company should consider the issue of legal privilege in this regard.

See Chapter 36 on privilege

Where boards are receiving legally privileged advice about investigations or material compliance issues, the way in which it is communicated to the board and documented in the minutes will need to be carefully managed. The GC100 Guidance on Directors' Duties states that directors should not be 'forced to evidence their thought processes' as this would create unnecessary process and 'inevitably expose directors to a greater and unacceptable risk of litigation'.

Duty to exercise independent judgment (section 173 CA 2006) 42.2.1.3

Directors must exercise independent judgment in the interests of their own company,[12] regardless of whether they align with the interests of other group companies. The principle that underpins this duty is that directors must not

11 http://www.frc.org.uk/document-library/financial-reporting-lab/2021/frc-lab-stakeholders-report-s-172.

12 CA 2006, s.173.

© Law Business Research 2021

subordinate their powers to the will of others unless they are authorised to do so under the constitution. Director nominees may therefore follow the instructions of their appointer if the company constitution so allows, provided that they are able to comply with their other legal obligations.

The duty does not prevent directors from seeking and relying on professional advice to form an opinion provided that the decision they reach is their independent judgment.[13] Directors may also delegate their powers (although they remain responsible for their exercise) provided that such a delegation is authorised.

Directors may also be able to fetter their discretion in certain circumstances, provided that it promotes the success of the company to do so. For example, directors could bind the company to an exclusive commercial arrangement and agree to exercise their powers to ensure that the contract was carried out.

42.2.1.4 Duty to exercise reasonable care, skill and diligence (section 174 CA 2006)

Directors must exercise reasonable care, skill and diligence in how they discharge their duties.[14] The standard is both objective (the care, skill and diligence that would reasonably be expected of a director acting with reasonable diligence) and subjective (the general knowledge, skill and experience that the particular director has). As a general rule, a non-executive director will not be expected to have the same level of knowledge of the internal workings of the business that an executive director would.

Directors must satisfy themselves that they have a proper understanding of the functions and duties of directors, the fundamental principles of company law, the company's business, the risks faced by the company and the regulatory and compliance regime in which it operates.[15] Directors should also, as a practical matter, ensure that they receive a proper induction and ongoing training to keep their knowledge, skills and experience up to date.

Directors may rely on the expertise of colleagues and advisers in discharging their functions. Indeed, a failure to seek expert advice may amount to a breach of the duty.[16] The right (or duty) to seek advice does not absolve a director from the duty to supervise the discharge of delegated functions.[17] It must be reasonable for directors to rely on the advice of colleagues or advisers.[18] For example, directors must ensure that advisers have appropriate expertise and are instructed to address relevant issues; they should also ensure that advisers are

13 *Duomatic Ltd, Re* [1969] 2 Ch. 365; [1969] 2 WLR 114; (1968) 112 SJ 922.

14 CA 2006, s.174(2) .

15 *Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig* [2017] All ER (D) 244.

16 *Duomatic Ltd* (see supra note 13).

17 *Bradcrown Ltd, Re* [2002] B.C.C. 428; [2001] 1 B.C.L.C. 547.

18 *Coleman Taymar Ltd v. Oakes* [2001] 2 B.C.L.C. 749.

© Law Business Research 2021

free from conflicts of interest.[19] The question of whether reliance is reasonable will depend on the circumstances.

Although there is no difference between the tests to be applied to executive and non-executive directors, the law recognises that because they fulfil different functions, they will reasonably be expected to exercise different levels of care, skill and diligence. The extent to which a non-executive director may reasonably rely on the executive directors would be fact-sensitive.[20] Non-executive directors should expect to comply with high standards. They would also be expected to properly understand any activity that contributed significantly to a company's commercial offering or revenues.[21]

Duty to avoid conflicts of interest (section 175 CA 2006) 42.2.1.5

Companies are entitled to the benefit of impartial decision-making on the part of their directors. Directors therefore have a duty to avoid actual and potential conflicts between their personal interests and those of the company they serve even where they are acting in good faith.[22] The duty is widely drawn. Section 175 of the CA 2006 states: 'A director of a company must avoid a situation in which he has, or can have, a direct or indirect interest that conflicts, or possibly may conflict, with the interests of the company.' The reference to indirect interests requires directors to take account of whether persons connected with them[23] might have a conflict of interest.

The application of the duty is acute where it involves the exploitation of a company's property, information or opportunity, and it is immaterial whether the company could itself have taken advantage of the opportunity or whether it suffered any loss. The test is an objective one and directors must therefore analyse whether a reasonable person would think that the relevant facts and circumstances gave rise to a real and sensible possibility of conflict. If the situation cannot reasonably be regarded as giving rise to a conflict of interest, the duty will not be breached.[24]

The duty will not be infringed where the conflict has been authorised in advance by the directors where there is a power to do so in the company's constitution.[25] The authorisation will only be effective if the relevant meeting is quorate without counting any interested directors and the authorisation was given without counting their votes. Effective authorisation will require

19 *Iesini v. Westrip Holdings Ltd* [2009] EWHC 2526 (Ch); [2010] B.C.C. 420; [2011] 1.

20 *Equitable Life Assurance Society v. Hyman* [2002] 1 A.C. 408; [2000] 3 WLR 529; [2001] Lloyd's Rep. IR 99.

21 *Continental Assurance Co of London Plc (In Liquidation), Re*; *Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig* [2017] All ER (D) 244; *Barings Plc (No. 5), Re, Secretary of State for Trade and Industry v. Baker* [1999] 1 B.C.L.C. 433.

22 CA 2006, s.175(1).

23 By reference to the list set out in CA 2006, s.252.

24 CA 2006, s.175(4)(a).

25 ibid., s.175(4)(b).

© Law Business Research 2021

directors to give full disclosure of the scope and nature of the conflict. In 2008, the GC100 published guidance on Directors' Conflicts of Interest, which includes guidance on authorisation.[26] Directors will not infringe their duties if they act in accordance with provisions in the company's articles for dealing with conflicts of interest.[27]

It may be possible for shareholders to authorise a conflict of interest in advance or subsequently ratify a breach of duty. There are limits on the type of conduct that can be authorised or ratified, and the process that applies will need to be checked taking into account the company's constitution.

42.2.1.6 Duty not to accept benefits from third parties (section 176 CA 2006)

Directors must not exploit their positions for personal benefit (financial or non-financial). The duty provides directors must not accept a benefit from a third party conferred by reason of them being a director or their doing (or not doing) anything as a director.[28] The duty will not be infringed if the acceptance of the benefit cannot reasonably be regarded as likely to give rise to a conflict of interest. The duty is very strict and directors need to take account of these obligations when accepting corporate hospitality or gifts. Although in a bribery investigation the focus will be on whether benefits provided to directors or the company were criminal, it is important not to lose sight of this duty where the conduct concerns individual directors. A company may recover the value of any benefits unlawfully received by a director through civil proceedings, and not just criminal action.

42.2.1.7 Duty to declare an interest in a proposed transaction or arrangement (section 177 CA 2006)

Section 177 CA 2006 requires a director to disclose to the other directors the nature and extent of any interest that the director has in relation to a proposed transaction or arrangement with the company. There is no requirement for authorisation. The term 'arrangement' is wider than the term 'transaction' and includes agreements or understandings having no contractual effect. The interest can be direct or indirect and therefore the interests of connected person must be considered.[29] Directors must disclose the nature and extent of the interest before the company enters into the transaction or arrangement.

Directors do not have to make a declaration where they are unaware of having an interest or are not aware of the transaction or arrangement in question. However, they will be assumed to have knowledge of matters of which they ought reasonably to be aware. Directors will therefore need to undertake

26 See also Chartered Governance Institute guidance on Directors' conflicts of interest.

27 CA 2006, s.180(4)(b).

28 ibid., s.176.

29 See ibid., s.252.

© Law Business Research 2021

a certain amount of due diligence regarding their potential interests to avoid breaching the duty.

If the interest cannot reasonably be regarded as likely to give rise to a conflict of interest, it need not be declared. Further, if the other directors are already aware, or ought reasonably to be aware, of the conflict of interest, it does not have to be declared. Finally, interests relating to a director's service contract need not be declared if they have been considered by a meeting of the directors or a committee appointed for the purpose.

The company's articles may contain provisions for dealing with conflicts of interest compliance that are designed to prevent a breach of the general duty.[30] Section 182 of the CA 2006 deals separately with declarations of interest in existing transactions or arrangements not already declared under section 177.[31]

Other statutory, common law and equitable duties 42.2.1.8

The statutory duties are not exhaustive. Directors of all UK companies also owe a duty of confidentiality to the company and have duties to act fairly as between different members and consider the interests of creditors in appropriate circumstances. Directors also have numerous reporting obligations. Other obligations will depend on the nature of the company.

UK Corporate Governance Code 42.2.2

Companies with premium listings in the United Kingdom are required (for accounting periods beginning on or after 1 January 2019) to state in their annual report and accounts whether they have complied with the UK Corporate Governance Code (2018)[32] and if not, explain the reason. The 'comply or explain' approach is designed to promote transparency about how companies have complied with the high standards of governance set out in the Corporate Governance Code and to promote trust.

The Corporate Governance Code (2018) is the latest iteration of a code that was first published in 1992. The revised code has been developed to respond to a modern business environment in which a key role of the directors is to build relationships with a wider group of stakeholders. The principles set out in the code have been updated to emphasise the link between strong corporate governance and long-term success.

The Corporate Governance Code is designed around five pillars:

- board leadership and company purpose;
- division of responsibilities;
- composition, succession and evaluation;

30 ibid., s.180(4)(b).

31 Breach of CA 2006, s.182 is a criminal offence.

32 https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf.

© Law Business Research 2021

- audit, risk and internal control; and
- remuneration.

The Corporate Governance Code sets out a number of principles in relation to each of these items. Although they are all relevant to the identification and management of financial crime risk and the investigation of issues arising, the principles linked to board leadership and company purpose, division of responsibilities, and audit, risk and internal control are the most relevant.

Principles relating to board leadership and company purpose require directors to act with integrity. They must ensure that they establish a framework of prudent and effective controls to assess and manage risk in which the workforce should be able to raise any matters of concern.

The principles linked to the division of responsibilities highlight that the chair should facilitate board relations and the effective contribution of all the non-executive directors. The chair should also ensure that directors receive accurate, timely and clear information. The board must ensure through its composition that no one individual or group dominates the board and that there is a clear division of responsibility between the leadership of the board and the executive leadership of the business.

The principles further provide that non-executive directors must have sufficient time to meet their responsibilities and 'should provide constructive challenge, strategic guidance, offer specialist advice and hold management to account'.[33] The company secretary should support the board to ensure that it has what it needs to function effectively and efficiently. This will include making time and proper information available to the board to discharge its oversight responsibilities.

The principles that underpin the section on audit, risk and internal control are of particular relevance in managing financial crime risk. They state:

> *M. The board should establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements.*
>
> *N. The board should present a fair, balanced and understandable assessment of the company's position and prospects.*
>
> *O. The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.*

33 Principle H, UK Corporate Governance Code.

© Law Business Research 2021

The audit committee is key in how the company complies with these obligations. The Corporate Governance Code sets out the requirements for the audit committee, which is responsible for, among other items:

> - *reviewing the company's internal financial controls and internal control and risk management systems, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself;*
> - *monitoring and reviewing the effectiveness of the company's internal audit function or, where there is not one, considering annually whether there is a need for one and making a recommendation to the board;*
>
> . . .
>
> - *reviewing and monitoring the external auditor's independence and objectivity;*
> - *reviewing the effectiveness of the external audit process, taking into consideration relevant UK professional and regulatory requirements*[34]

The board retains overall responsibility for assessing and managing the company's risks. Boards must carry out a robust assessment of the company's emerging and principal risks, have in place procedures to identify its emerging risks and explain how these are being managed or mitigated. The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

Separately, the FRC has published Guidance on Audit Committees,[35] Guidance on Audit Quality[36] and Guidance on Risk Management, Internal Control and Related Financial and Business Reporting[37] to assist companies in complying with these principles.

Appendix C of the Guidance on Risk Management, Internal Control and Related Financial and Business Reporting sets out the questions the board can ask itself in the context of its risk-related responsibilities, as the small sample of its risk-related questions set out below illustrates:

> *Risk appetite and culture*
>
> - *How has the board agreed the company's risk appetite? With whom has it conferred?*

34 Provision 25, UK Corporate Governance Code.

35 https://www.frc.org.uk/getattachment/6b0ace1d-1d70-4678-9c41-0b44a62f0a0d/Guidance-on-Audit-Committees-April-2016.pdf.

36 https://www.frc.org.uk/getattachment/68637e7a-8e28-484a-aec2-720544a172ba/Audit-Quality-Practice-Aid-for-Audit-Committees-2019.pdf.

37 https://www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf.

© Law Business Research 2021

- *How has the board assessed the company's culture? In what way does the board satisfy itself that the company has a 'speak-up' culture and that it systematically learns from past mistakes?*
- *How do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control systems?*
- *How has the board considered whether senior management promotes and communicates the desired culture and demonstrates the necessary commitment to risk management and internal control?*
- *How is inappropriate behaviour dealt with? Does this present consequential risks?*
- *How does the board ensure that it has sufficient time to consider risk, and how is that integrated with discussion on other matters for which the board is responsible?*

. . .

Monitoring and Review

- *What are the processes by which senior management monitor the effective application of the systems of risk management and internal control?*
- *In what way do the monitoring and review processes take into account the company's ability to re-evaluate the risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?*
- *How are processes or controls adjusted to reflect new or changing risks, or operational deficiencies? To what extent does the board engage in horizon scanning for emerging risks?*

Public reporting

- *How has the board satisfied itself that the disclosures on risk management and internal control contribute to the annual report being fair, balanced and understandable, and provide shareholders with the information they need?*
- *How has the board satisfied itself that its reporting on going concern and the longer term viability statement gives a fair, balanced and understandable overview of the company's position and prospects?*

The UK Corporate Governance Code does not override or seek to interpret the general duty under section 172 of the CA 2006 to promote the success of the company. However, it is clear from the above that many of the suggestions for how to identify and manage risk will apply in both the context of the general section 172 duty and also the duty to exercise reasonable care, skill and diligence.

© Law Business Research 2021

QCA Code for smaller listed companies 42.2.3

The QCA Corporate Governance Code[38] is intended to provide small and mid-sized UK quoted companies with a corporate governance framework tailored to their needs and less prescriptive than the UK Corporate Governance Code. It consists of 10 corporate governance principles that companies should follow, along with step-by-step guidance on how to effectively apply them and the related disclosures companies should make.

The 10 principles are to:

- establish a strategy and business model which promote long-term value for shareholders;
- seek to understand and meet shareholder needs and expectations;
- take into account wider stakeholder and social responsibilities and their implications for long-term success;
- embed effective risk management, considering both opportunities and threats, throughout the organisation;
- maintain the board as a well-functioning, balanced team led by the chair;
- ensure that between them the directors have the necessary up-to-date experience, skills and capabilities;
- evaluate board performance based on clear and relevant objectives, seeking continuous improvement;
- promote a corporate culture that is based on ethical values and behaviours;
- maintain governance structures and processes that are fit for purpose and support good decision-making by the board; and
- communicate how the company is governed and is performing by maintaining a dialogue with shareholders and other relevant stakeholders.

Since September 2018, companies listed on the Alternative Investment Market[39] have been required to adopt and identify a recognised corporate governance code. Companies are also required to set out how they comply with that code or explain their reasons for non-compliance.[40]

Wates Corporate Governance Principles for Large Private Companies 42.2.4

In recent years, the government has extended its focus on corporate governance to large private companies. This is in recognition that private companies are both a substantial and an expanding part of the economy. Under the leadership of the Wates Committee, the FRC and others have developed the

38 https://www.theqca.com/shop/guides/143861/corporate-governance-code-2018-downloadable-pdf.thtml.

39 AIM – the international market for smaller, growing companies operated by the London Stock Exchange.

40 AIM Rules, Rule 26.

© Law Business Research 2021

Wates Corporate Governance Principles for Large Private Companies.[41] The guidance sets out six principles that such companies should consider within the context of the company's specific circumstances and then explain how they have addressed them in their governance practices. The guidance exists to assist companies but does not have the same status as the UK Corporate Governance Code, which requires companies to comply or explain why they have not done so.

The two principles most relevant to financial crime investigations are Principles 3 (Director responsibilities) and 4 (Opportunity and risk). Principle 3 requires the board and individual directors to have a clear understanding of their accountability and responsibilities. Principle 3 states that the board's policies and procedures should support effective decision-making and independent challenge. The responsibility of reviewing the governance processes to confirm that they remain fit for purpose and considering any initiatives that could strengthen the governance of the company reside with the chairman and company secretary. The guidance also emphasises the importance of the integrity of information and that the board papers and supporting information should inform the director what is expected of them on each issue.

Principle 4 states that the board is responsible for a company's overall approach to strategic decision-making and both financial and non-financial risk management, including reputational risk. The board must have oversight of risk and how it is managed, and provide appropriate accountability to stakeholders: 'The size and nature of the business will determine the internal control systems put in place to manage and mitigate both emerging and principal risks. Some companies may decide to delegate to a committee to oversee such matters.'

The guidance further elaborates on the responsibilities of the board as follows:

> *The board should establish an internal control framework with clearly defined roles and responsibilities for those involved. It should agree an approach to reporting, including frequency of reporting and the points at which decisions are made and escalated. Responsibilities may include:*
>
> - *developing appropriate risk management systems that identify emerging and established risks facing the company and its stakeholders. Such systems should enable the board to make informed and robust decisions, including those associated with material environmental, social and governance matters, such as climate change, workforce relationships, supply chains, and ethical considerations;*

41 https://www.frc.org.uk/getattachment/31dfb844-6d4b-4093-9bfe-19cee2c29cda/Wates-Corporate-Governance-Principles-for-LPC-Dec-2018.pdf.

© Law Business Research 2021

- *determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite');*
- *agreeing how the principal risks should be managed or mitigated and over what timeframe to reduce the likelihood of their incidence or the magnitude of their impact;*
- *establishing clear internal and external communication channels on the identification of risk factors, both internally and externally; and*
- *agreeing a monitoring and review process.*

FRC Guidance on Board Effectiveness 42.2.5

In July 2018, the FRC published its revised non-mandatory and non-prescriptive Guidance on Board Effectiveness[42] to assist boards to understand and consider good practice in the context of their corporate governance obligations. The Guidance on Board Effectiveness adopts the same structure as the Corporate Governance Code. However, there is not space in this chapter to summarise the good practices identified, other than to note that it places a strong emphasis on tone from the top and the continual monitoring of culture. Two important sources of cultural data identified are (1) whistleblowing, grievance and 'speak-up' data and (2) attitudes to regulators, internal audit and employees. The Guidance on Board Effectiveness also suggests taking an integrated approach, noting that resources, internal audit, risk and compliance all have a role to play. Providing examples of questions the board can pose itself on different issues, the Guidance on Board Effectiveness is a rich source of information for those assisting a company with remediation or cultural transformation in the context of an investigation (or outside the investigative process).

Reporting on section 172 compliance and corporate governance generally 42.2.6

The CA 2006 requires that all companies, other than those entitled to the small companies' exemption, prepare a stand-alone strategic report. The FRC has clarified that the requirement to produce a strategic report includes companies that are categorised as 'medium-sized' under section 465 CA 2006 but are excluded from being treated as such because they are ineligible under section 467 CA 2006.[43] The statutory purpose of the strategic report is to 'inform the members of the company and help them assess how directors have performed their duty' under section 172 (duty to promote the success of the company for the benefit of members as a whole) and in doing so to have regard to the non-exhaustive range of stakeholder interests and other considerations

42 https://www.frc.org.uk/getattachment/61232f60-a338-471b-ba5a-bfed25219147/2018-Guidance-on-Board-Effectiveness-FINAL.PDF.

43 https://www.frc.org.uk/getattachment/3a35133f-47a0-4145-a041-a60c66e633e5/Amendments-cover-May-2020.pdf.

© Law Business Research 2021

set out in that section. The strategic report must include an explanation of the principal risks and uncertainties faced by the business and disclose information about a number of issues, including material anti-corruption and anti-bribery issues.

Since 2007, when it first came into force, section 172 has, therefore, enshrined the importance of the consideration of wider interested groups in the creation of a successful business for the benefit of shareholders. However, in light of a number of high-profile examples of poor corporate governance – where there was little evidence that appropriate regard had been had to the needs of a broader range of stakeholders (including employees, suppliers and pension beneficiaries) – the government brought forward The Companies (Miscellaneous Reporting) Regulations 2018 (Reporting Regulations) to fulfil its commitment to strengthen stakeholder voices in boardroom decision-making.

The Reporting Regulations aim to drive greater transparency by requiring companies who must prepare a strategic report (other than those that qualify as medium-sized) to ensure that their strategic reports for each year beginning on or after 1 January 2019 include a statement describing how directors have had regard to the matters set out in section 172(1), paragraphs (a) to (f) of the CA 2006 when performing their duties under that section. All qualifying companies, including subsidiaries, must report and publish their section 172(1) statements on their websites, whether separately or as part of their annual report. The FRC has revised its Guidance on the Strategic Report accordingly.

The Reporting Regulations also amend the content requirements of the directors' report to require certain companies (meeting different qualifying criteria) to include a basic level of information on their stakeholder engagement. This includes disclosing how the board has had regard to the interests of its UK employees and to the need to foster the company's business relationships with suppliers, customers and others and, in both cases, explaining the effect, including on the principal decisions taken by the company during the financial year.

While there is a degree of overlap between the section 172(1) statements and the revised content requirements for the directors' report, the government's guidance[44] clarifies that the latter requirements are designed to ensure that company reporting includes information about the 'important aspects of the section 172(1) duty even where directors do not judge the information to be of sufficient strategic importance to be included in the strategic report that year'. Where the board considers its stakeholder engagement information is of strategic importance, it may choose to include that information in its strategic report and not its directors' report, with appropriate cross-referencing in the directors' report.

44 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755002/The_Companies__Miscellaneous_Reporting__Regulations_2018_QA_-_Publication_Version_2__1_.pdf.

© Law Business Research 2021

The Reporting Regulations also impose further enhanced reporting obligations as regards governance arrangements on very large UK-incorporated companies, including subsidiaries, with either more than 2,000 employees globally, or an annual turnover over of £200 million globally and a balance sheet total over £2 billion globally. Premium and standard listed companies which are already required to report on their corporate governance arrangements under the Financial Conduct Authority's (FCA) Disclosure Guidance and Transparency Rules (DTR) 7.2 are not within scope.[45] Premium listed companies are required to apply, and comply or explain their non-compliance with, the provisions of the UK Corporate Governance Code under the FCA's Listing Rules.[46]

Companies in scope must include a statement as part of their directors' report stating which corporate governance code, if any, has been applied and how. If the company has departed from the code, it must set out the respects in which it has done so, and the reasons. If the company has not applied any corporate governance code, the statement must explain why and what arrangements for corporate governance were applied. Statements must also be published on a website maintained by or on behalf of the company.

Adherence to the UK Corporate Governance Code remains under scrutiny. In the FRC's Review of Corporate Governance Reporting in November 2020, it noted that while some companies have embraced the opportunities that the 2018 iteration of the UK Corporate Governance Code presented to report to their stakeholders in a way that allows them to communicate about how their governance functions to deliver the company's purpose and strategy, some companies continue to treat the Code as a box-ticking exercise, with formulaic reporting that does not meaningfully explain why they do not comply with its provisions.[47]

Senior managers regime 42.2.7

The PRA's and FCA's new regime for supervising and approving the conduct of individuals in regulated firms, the SMCR replaces and extends the previous oversight rules for individuals, the Approved Persons Regime. This is a response to the perceived 'firewall of accountability' protecting senior management from

45 Community interest companies and charitable companies are also exempted.

46 The FCA has published new proposals on climate-related disclosure rules for listed companies and certain regulated firms. The FCA is proposing to extend the application of Taskforce on Climate-related Financial Disclosures (TCFD) for premium-listed commercial companies to issuers of standard listed equity shares and to introduce TCFD-aligned disclosure requirements for asset managers, life insurers and FCA-regulated pension providers. The FCA invited feedback to both consultations by 10 September 2021 and is seeking feedback on a draft technical note setting out further guidance on its disclosure expectations.

47 https://www.frc.org.uk/document-library/corporate-governance/2020/corporate-governance-review-2020.

© Law Business Research 2021

regulatory enforcement. The SMCR is intended to clarify and enhance the division of responsibilities in firms, improve the conduct of all staff and to make disciplinary action against individuals easier for the PRA and FCA (the regulators).[48]

The SMCR regulates individuals in three segments, divided roughly according to seniority:

- Senior managers are the most senior individuals responsible for managing aspects of a firm's affairs that risk serious consequences for the firm or business in the United Kingdom.[49]
- Certification regulates other individuals in firms who the FCA considers conduct types of roles that carry a risk of significant harm to consumers or the market.[50]
- The conduct rules govern the behaviour of all other employees within firms whose roles relate to regulated or unregulated financial services activity.

There is no territorial limit, so the SMCR can capture individuals based overseas, and is not limited to employees.

Banks, insurers and the largest FCA regulated firms must also submit to the regulators a very detailed 'responsibilities map' of senior individuals, oversight, governance and reporting lines, and a statement of responsibilities for each senior management function manager (SMF manager) setting out what matters that individual is responsible for. The documents must explain to whom certain standard 'prescribed responsibilities' designated by the regulators have been allocated. These documents must be kept up to date.

Only SMF managers are now approved as fit and proper by the regulators: in contrast to the previous approved persons regime, certified persons (who will in many cases include individuals previously approved by the FCA) will now only be certified as fit and proper by their employer firms, not the regulators. Firms must test and confirm the fitness and propriety of SMF managers and certified staff annually. This is likely to lead to more employment claims from staff who lose their certification.

The regulators can take disciplinary action against individuals in any of these three categories for breach of the conduct rules or for being 'knowingly concerned' in the firm's breach of the regulators' rules. In addition to

48 Firms caught by the Senior Managers and Certification Regime will either report solely to the FCA (solo-regulated) or to both the FCA and PRA (dual-regulated). A firm's reporting route will depend on whether it is dual- or solo-regulated.

49 The description set out in s.59ZA, Financial Services and Markets Act 2000 as amended Financial Services (Banking Reform) Act 2013. This is the legislative provision empowering the PRA and FCA to designate senior manager functions.

50 This paraphrases the description set out in s.63E of the Financial Services and Markets Act 2000 (as amended, ibid.), which is the legislative provision empowering the PRA and FCA to designate certification functions.

© Law Business Research 2021

the previous 'knowing concern' test, there is a new statutory test[51] for taking action against a senior manager where (1) the firm breaches a regulatory rule or requirement, (2) the senior manager was at the time responsible for the activities of the firm where the breach occurred, and (3) the senior manager failed to take reasonable steps to prevent or stop the breach occurring. The test imposes a 'duty of responsibility' on senior managers, which has made the record-keeping of decisions and execution of duties more important.

Complementary rules on handover arrangements where senior managers depart, notifications of breaches to the regulators, and requirements for detailed regulatory references when certified or senior management staff leave a firm are designed to enhance the effectiveness of the Regime.

The SMCR came into force in full for banks in 2018 and insurers in 2019. For all other FCA regulated firms, the senior manager provisions of the SMCR rules came into force on 9 December 2019, and firms were also required by this date to have identified their certification staff. The obligation to certify staff and the application of the individual conduct rules were originally intended to come into force on 9 December 2020. In response to the covid-19 pandemic, the FCA delayed the deadline for firms to have undertaken the first certification process and the date that the Individual Conduct Rules came into force (and the date therefore by which employees must have conducted relevant training and breach notification requirements must have been in place) was pushed back until 31 March 2021.

In addition, to reflect the absence of certified persons from the FCA register under the new regime, the FCA has created a new public directory of certified individuals. The deadline for reporting individuals to be included in the directory was also extended to 31 March 2021 to reflect the extension of time for certifying them.[52] However, the FCA has stressed that firms should comply with the original deadline of 9 December 2020, where possible.

Consequences of breach

The potential consequences for staff subject to the conduct rules who are found by the relevant regulator to have engaged in misconduct or market abuse include a private warning, public censure, unlimited financial penalty, and in the case of SMF managers a restriction, suspension or prohibition from being an approved person. While some forms of directors' and officers' insurance cover the costs of representing an individual in an investigation, the FCA has drafted rules to ensure a financial penalty is paid by the person on whom it is imposed. GEN 6.1.4A of the FCA Handbook prohibits a regulated firm from paying any financial penalty imposed on an employee, director or partner of the firm or of an affiliated company. GEN 6.1.5 is widely drafted to prohibit

See Chapter 13 on employee rights

51 In the Financial Services and Markets Act 2000 (as amended), s.66A.

52 https://www.fca.org.uk/publication/consultation/cp20-10.pdf.

© Law Business Research 2021

insurance arrangements designed to indemnify any person against all or part of a financial penalty.

42.3 Expectations, not obligations

A recent judgment handed down in the context of approving a deferred prosecution agreement[53] illustrates changing expectations of how boards will behave where internal investigations identify evidence of possible criminal conduct. In this case the company had no obligation to self-report concerns about misconduct and chose not to do so. The judge observed that:

> *the main Board . . . was primarily concerned to minimise the adverse consequences of the offending for the Group. In my judgment the proper course for it to have adopted, not as a matter of legal duty, but as a matter of ethical corporate governance was to report the known facts to the SFO. . . . I accept that there was no legal requirement to report suspected crime to the authorities, but there is a moral duty on all citizens in this respect which extends at least equally to corporations. This failure by the Board of FWL was deplorable.*

These comments are interesting for numerous reasons. In the context of this chapter we will limit our remarks to noting that the judge's observations are not binding law but do illustrate the changing expectations in respect of board behaviour, and the risk of judicial criticism where they are not met.

42.4 Conclusion

There are many and varied sources of corporate governance obligations and related duties on boards and companies. Although the standards expected of the board as a collective and directors individually will vary depending on the company (listed, regulated, subject to the SMCR, large, complex and so on) and the issues involved, there is considerable convergence in relation to the types of behaviour that are regarded as constituting good practice for identifying and managing risk (including financial crime risk). Directors must ensure that they understand their duties and obligations and their application to their compliance oversight obligations.

53 *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep. FC Plus 27.

© Law Business Research 2021

43

Directors' Duties: The US Perspective

Daniel L Stein, Jason Linder, Glenn K Vanzura and Bradley A Cohen[1]

Introduction 43.1

As stewards of the corporation and fiduciaries of its shareholders, directors are primarily responsible for overseeing the company's business and affairs. In exercising these responsibilities, directors must discharge their fiduciary duties of care and loyalty and their obligation to act in good faith. Directors, however, confront mounting litigation and regulatory risk in navigating their fiduciary duties and the demands of shareholders in the face of corporate compliance crises and independent investigations. In addition, regulators in the United States and around the world have become increasingly focused on the role of the board and its directors with respect to corporate governance, financial reporting and promoting a culture of compliance. In this chapter, we discuss the fiduciary duties owed by directors in the context of independent investigations, potential director liability for violations of those duties, and strategic considerations for directors to satisfy their fiduciary duties when faced with compliance crises.[2]

Directors' fiduciary duties 43.2

In the United States, the fiduciary duties and responsibilities of members of boards of directors arise primarily out of state corporate law, both from state

1 Daniel L Stein, Jason Linder and Glenn K Vanzura are partners, and Bradley A Cohen is an associate, at Mayer Brown. The authors would like to acknowledge the work of Timothy P O'Toole, William P Barry and Margot Laporte of Miller & Chevalier Chartered for the fourth edition of this volume and on which this present chapter is based.

2 Directors also face potential liability for breaches of fiduciary duties in other contexts beyond independent investigations, such as those arising in the mergers and acquisitions context, though a discussion of such duties falls beyond the scope of this chapter.

© Law Business Research 2021

statutes and evolving case law.[3] Fundamentally, directors owe fiduciary duties of care and loyalty to the corporation and are expected to carry out their obligations in good faith.[4] These duties are an essential part of a director's oversight and stewardship responsibilities to the corporation.

43.2.1 Duty of care

The duty of care requires directors to exercise the proper amount of care as they make business decisions on behalf of their corporation. Directors must act with that amount of care which ordinarily careful and prudent people would use in similar circumstances, and consider all material information reasonably available in making business decisions.[5] Therefore, to fulfil their duty of care, directors must, among other things: be knowledgeable about the corporation, its business, its industry and relevant risks, including by regularly reviewing financial statements and inquiring into corporate affairs; remain informed about decisions faced by the board; and engage in meaningful deliberation of issues that arise.[6] If a director 'feels that he has not had sufficient business experience to qualify him to perform the duties of a director, he should either acquire the knowledge by inquiry, or refuse to act [as a director]'.[7]

Director liability for breaching the duty of care typically arises in two contexts: (1) grossly negligent board decisions that result in a loss for the corporation; and (2) liability for a loss that arose from an 'unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss'.[8] In *Smith v. Van Gorkom*, the Delaware Supreme Court found that the directors of Trans Union Corporation had breached their duty of care by acting with gross negligence in failing to make an informed decision regarding the sale of the company.[9] The Delaware Supreme Court cited the

3 While civil liability for breaches of fiduciary duties arises under state law, public company directors separately may face federal criminal and civil liability for violations of the federal securities laws. For example, among other violations, public company directors may be held liable for financial reporting and disclosure violations, and insider trading and other fraud violations, under the Securities Act of 1933 [Securities Act] and the Securities Exchange Act of 1934 [Exchange Act]. The Sarbanes-Oxley Act of 2002 [Sarbanes-Oxley] and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 also enhanced director liability under federal law for self-dealing and compensation-related violations, among others.

4 *In re Walt Disney Co. Derivative Litig.*, 907 A.2d 693, 745 (Del. Ch. 2005), aff'd, 906 A.2d 2 (Del. 2006) (*Disney*).

5 Id. at 749 (internal quotation marks omitted).

6 See *Francis v. United Jersey Bank*, 432 A.2d 814, 822 (N.J. 1981) (duty to conduct regular review of financial statements); *Barnes v. Andrews*, 298 F. 614, 615 (S.D.N.Y. 1924) (duty to enquire into the corporate business).

7 *Francis*, 432 A.2d at 822 (internal quotation marks omitted).

8 *Disney*, 907 A.2d at 749 (quoting *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996) [*Caremark*] (alterations omitted)).

9 *Smith v. Van Gorkom*, 488 A.2d 858, 881 (Del. 1985).

© Law Business Research 2021

board's approval of the sale without having reviewed a term sheet or any other documentation to support the adequacy of the sale price, and that the board relied, without any basis, on the uninformed statements of a director regarding the proposed agreement.[10]

Directors are only liable for breach of the duty of care if their conduct is grossly negligent, meaning that they demonstrated a 'reckless indifference to or a deliberate disregard of the whole body of stockholders or actions which are without the bounds of reason'.[11] Courts have found that 'directors' actions need not achieve perfection to avoid liability', and that directors do not breach a legal duty simply because they 'failed to act as a model director might have acted'.[12] In general, monetary damages are unavailable to plaintiffs alleging breach of the duty of care, even if they can demonstrate gross negligence, since many states, in response to *Van Gorkom*,[13] enacted statutes permitting corporations to eliminate or limit directors' personal liability for monetary damages for breaches of their duty of care.[14] Significantly, these state laws do not authorise corporations to eliminate or limit directors' personal liability for breaches of their duty of loyalty or good faith obligations, and monetary damages remain available to plaintiffs for such breaches.[15]

Duty of loyalty 43.2.2

The duty of loyalty 'mandates that the best interest of the corporation and its shareholders take precedence over any interest possessed by a director, officer or controlling shareholder and not shared by the stockholders generally'.[16] Directors are also prohibited from using their position of trust and confidence to further their private interests.[17]

As a 'subsidiary element' of the duty of loyalty, directors must carry out their duties in 'good faith'.[18] The obligation to act in good faith is not an independent fiduciary duty or direct basis for liability, but rather is at the core of the duty of loyalty – 'a director cannot act loyally towards the corporation unless she acts

10 Id. at 874.

11 *Disney*, 907 A.2d at 750 (internal quotations marks omitted).

12 *Cooke v. Oolie*, Civ. Action No. 11134, 2000 Del. Ch. LEXIS 89, at *58–59 (Del. Ch. 24 May 2000).

13 *Disney*, 907 A.2d at 751.

14 See, e.g., Del. Code Ann. tit. 8, § 102(b)(7). In states that have enacted statutes in response to *Van Gorkom*, plaintiffs may still seek equitable remedies such as injunctive relief; in those states, however, directors may be protected from monetary liability where their corporation, in its by-laws or otherwise, has eliminated or limited its directors' personal liability for monetary damages for breaches of their duty of care. See, e.g., *Arnold v. Society for Sav. Bancorp, Inc.*, 678 A.2d 533 (Del. 1996).

15 See, e.g., Del. Code Ann. tit. 8, § 102(b)(7).

16 *Disney*, 907 A.2d at 751 (internal quotation marks and alteration omitted).

17 *Guth v. Loft, Inc.*, 5 A.2d 503, 510 (1939).

18 *Stone v. Ritter*, 911 A.2d 362, 369 (Del. 2006).

© Law Business Research 2021

in the good faith belief that her actions are in the corporation's best interest'.[19] A director fails to act in good faith where the director 'intentionally acts with a purpose other than that of advancing the best interests of the corporation, where [the director] acts with the intent to violate applicable positive law, or where [the director] intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for [his or her] duties'.[20]

Courts have interpreted the duty of loyalty as giving rise to the duty to exercise oversight in the day-to-day business operations of the corporation. The Delaware Court of Chancery set forth the standard for directors' obligation to oversee and monitor the corporation in *In re Caremark International Inc. Derivative Litigation*, holding that directors have an affirmative duty to establish a reporting system and internal controls, and to monitor and oversee internal compliance activity.[21] Directors must ensure that the system of internal controls is 'reasonably designed' to allow senior management and the board to reach 'informed judgments concerning both the corporation's compliance with law and its business performance'.[22] Failure to do so, the court held, may 'render a director liable for losses caused by non-compliance with applicable legal standards'.[23]

Thus, while 'directors' good faith exercise of oversight responsibility may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability or both',[24] directors are expected to take steps to implement reasonable reporting, information and compliance systems, and to address known instances of corporate misconduct.[25]

43.2.3 Oversight obligations under US securities laws

In addition to the standards articulated in *Caremark* and its progeny, the Sarbanes-Oxley Act of 2002 established expectations for public company audit committees (and consequently the independent directors that serve on audit committees) with respect to their oversight of companies' accounting, internal controls and auditing matters. These include oversight of the company's independent auditors, review of audit reports and the establishment of procedures to address complaints regarding the company's accounting and financial reporting.[26] Audit committees may also hire independent counsel to assist them in fulfilling their responsibilities, including in independent audit committee investigations and compliance assessments.[27]

19 Id. at 370.

20 Id. at 369.

21 *Caremark*, 698 A.2d at 970.

22 Id.

23 Id.

24 *Stone*, 911 A.2d at 373.

25 Id. at 370.

26 Sarbanes-Oxley, Pub. L. No. 107-204, 116 Stat. 745, § 301.

27 Id.

© Law Business Research 2021

Liability for breach of fiduciary duties 43.3

Caremark claims in private civil actions 43.3.1

Directors who allegedly breach their fiduciary duties may be subject to civil action in their personal capacity by shareholders of the corporation, both directly and in derivative lawsuits on behalf of the corporation. Courts determine liability on a director-by-director basis, as opposed to the conduct of the board as a whole.[28] In the majority of US states, the remedy for breach of a fiduciary duty can be 'Any form of equitable and monetary relief'[29] that the court finds 'appropriate'.[30]

Caremark established the standard of liability for alleged breaches of directors' duty of oversight, holding that 'only a sustained or systemic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability'.[31] *Caremark*, therefore, 'articulates a standard for liability for failures of oversight that requires a showing that the directors breached their duty of loyalty by failing to attend to their duties in good faith'.[32] In order to establish liability, plaintiffs must demonstrate that 'the directors were conscious of the fact that they were not doing their jobs'.[33]

In *Stone v. Ritter*, the Delaware Supreme Court affirmed the *Caremark* standard for oversight liability,[34] holding that a claim for director oversight liability requires the following conditions predicate: (1) that the directors 'utterly failed to implement any reporting or information system or controls'; or (2) that the directors, 'having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention'.[35] In either case, plaintiffs must demonstrate that directors knowingly violated their fiduciary obligations to hold them liable for such a claim.[36]

While *Caremark* and *Stone* set a high bar for establishing liability for breach of oversight obligations, board processes and decision-making can nonetheless result in director liability. For example, in the *Wells Fargo & Co Shareholder Derivative Litigation*, plaintiffs alleged that the defendant directors 'knew or consciously disregarded' that Wells Fargo employees were fraudulently

28 *Disney*, 907 A.2d at 748.

29 *In re Tri-Star Pictures, Inc. Litig.*, 634 A.2d 319, 333 (Del. 1993) (internal quotation marks omitted).

30 *Cinerama, Inc. v. Technicolor, Inc.*, 663 A.2d 1156, 1166 (Del. 1995) (internal quotation marks omitted). Often, directors' liability for monetary payments will be covered by directors and officers liability insurance.

31 *Stone*, 911 A.2d at 369 (internal quotation marks omitted).

32 *Guttman v. Huang*, 823 A.2d 492, 506 (Del. Ch. 2003).

33 Id.

34 *Stone*, 911 A.2d at 369.

35 Id. at 370.

36 Id.

© Law Business Research 2021

creating millions of deposit and credit card accounts for customers as part of 'cross-selling' activities.[37] In denying Wells Fargo's motion to dismiss, the court relied on allegations that the board had been informed of multiple 'red flags' of improper conduct, including alleged communications between employees and board members regarding the fraudulent activity, several related lawsuits, news reports, investigations by government agencies, employee terminations allegedly aimed at silencing whistleblowers, and emphasis on the importance of cross-selling practices in the bank's financial reports.[38] The court found that the numerous red flags alleged 'collectively supported an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and that there is a substantial likelihood of director oversight liability'.[39]

43.3.2 The business judgment rule

Directors' actions are generally shielded by the 'business judgment rule', a standard of judicial review that protects directors from personal civil liability for their decisions to the extent that the decision was independent, informed and made in good faith, with due care and with the honest belief that the action taken was in the company's best interest.[40] The business judgment rule presumes that 'in making a business decision the directors of a corporation acted on an informed basis, . . . and in the honest belief that the action taken was in the best interests of the company [and its shareholders]'.[41]

Therefore, the business judgment rule presupposes that directors have satisfied their duty of loyalty to the corporation. In the absence of evidence to the contrary, the board's 'decision will be upheld unless it cannot be attributed to any rational business purpose'.[42] Plaintiffs that fail to rebut this presumption will not be entitled to any remedy unless the transaction constitutes corporate waste.[43] To rebut this presumption, plaintiffs must demonstrate that the directors breached either their duty of loyalty or duty of care in connection with the transaction at issue.[44] In that instance, the burden shifts to the directors to demonstrate that the challenged transaction was 'entirely fair to the corporation and its shareholders'.[45]

Even if directors have exercised their business judgment, the business judgment rule will not protect directors who have made an 'unintelligent or

37 *In re Wells Fargo & Co. S'holder Derivative Litig.*, 282 F. Supp. 3d 1074, 1082 (N.D. Cal. 2017) (Wells Fargo).

38 Id. at 1088.

39 Id. (alterations omitted); see also id. at 1107–09.

40 *See Gantler v. Stephens*, 965 A.2d 695, 705–06 (Del. 2006).

41 *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984).

42 *Disney*, 907 A.2d at 747 (internal quotation marks omitted).

43 Id.

44 Id.

45 Id.

© Law Business Research 2021

unadvised judgment'.[46] Furthermore, the protections of the business judgment rule will not apply in the event of director inaction, absent a conscious decision not to act.[47] Accordingly, boards and directors should work with management to develop a process that (1) enables the board to obtain the information it needs to evaluate and decide on a course of action, (2) facilitates careful consideration and debate at the board level consistent with directors' fiduciary obligations and (3) results in a record that illustrates the board's execution of its responsibilities.

Regulatory enforcement actions 43.4

In addition to being named in securities class action or derivative suits, directors of public companies can be subjected to regulatory investigations and enforcement actions under US securities laws. Directors increasingly face all three proceedings – securities class actions, derivative litigation and enforcement proceedings – in parallel. Since one type of proceeding often leads to another type alleging the same conduct or inaction, a director's exposure to liability from a breach of fiduciary duties can multiply.

The Securities Exchange Act of 1934 (the Exchange Act), as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act), authorises the US Securities and Exchange Commission (SEC) to institute administrative and civil proceedings and to seek monetary and injunctive relief from directors for their violations of the securities laws.[48] The SEC also can seek a court order permanently or temporarily barring an individual from serving as a public company officer or director for violations of the anti-fraud provisions of the US securities laws.[49] Additionally, the US Department of Justice (DOJ) can criminally prosecute directors for 'willful' or 'knowing' violations[50] of the US securities laws or conspiracy to commit such violations.[51]

US regulators may impose clear and direct consequences against companies whose oversight they determine to be lacking. In evaluating corporate compliance programmes, regulators focus on the types of information that the board has examined in its exercise of oversight in the area in which misconduct occurred. US regulators have been vocal in commenting on the roles and responsibilities of directors and have been critical of boards of directors that,

46 Id. at 748 (internal quotation marks omitted).

47 Id.

48 Exchange Act §§ 21(a)(1), (d)(3), (d)(5), 15 U.S.C. §§ 78u(a)(1), (d)(3), (d)(5).

49 Id. § 21(d)(2), 15 U.S.C. § 78u(d)(2).

50 Securities Act § 24, 15 U.S.C. § 77x; Exchange Act §§ 13(a), 32(a), 15 U.S.C. §§ 78m(b)(4) and (5), 78ff(a). The securities laws define 'knowing' violations as being 'aware' that one is engaging in conduct, that circumstances exist, or that a result is substantially certain to occur, or having a firm belief of the same. 15 U.S.C. § 78dd-1(f).

51 Sarbanes-Oxley § 902(a), 18 U.S.C. § 1349.

© Law Business Research 2021

in their view, fail to exercise reasonable oversight.[52] The SEC and DOJ have been particularly outspoken with respect to financial reporting and Foreign Corrupt Practices Act (FCPA) matters. For instance, in a 2017 settlement with Sociedad Química y Minera de Chile (SQM) for internal controls and books-and-records violations under the FCPA, the DOJ explicitly noted that although SQM's board had been briefed on certain internal controls failures flagged by internal audit, 'no adequate changes were made to SQM's internal accounting controls'.[53]

Section 20(a) of the Exchange Act is particularly relevant to public company directors, as it provides that every person who indirectly or directly controls another person found liable for a securities violation under the Exchange Act is liable for that same conduct.[54] For 'control person' liability to attach, the majority of US circuit courts require only that the director exercised control over the general operations of the business that included the violation and could exercise control over the transaction or activity giving rise to it.[55] Section 20(a) provides an affirmative defence to a director who 'acted in good faith' and 'did not directly or indirectly induce' the act constituting the violation.[56]

For example, in 2009, the SEC filed a settled enforcement action against Nature's Sunshine Products, its chief executive officer (CEO) and board member, and its chief financial officer (CFO), alleging that the CEO/director and CFO, in their capacities as control persons under Section 20(a), violated the books-and-records and internal controls provisions of the FCPA.[57] Notably, the SEC did not allege that these individuals had direct knowledge of, or participated in, the underlying improper payments or accounting failures, but rather that the executives failed to identify certain red flags that would have alerted them to the improper payments and failed to perform their corporate duties adequately and in good faith.[58]

---

52 See, e.g., Mary Jo White, Chair, US Securities and Exchange Commission, Address at the Stanford University Rock Center for Corporate Governance: A Few Things Directors Should Know About the SEC (23 Jun. 2014) ('One question we are often asked is whether some of the things we are doing may actually discourage strong directors from serving on boards because of the risk that they may unfairly find themselves on the wrong end of an SEC enforcement action. While we do bring cases against directors, these cases should not strike fear in the heart of a conscientious, diligent director').

53 *United States v. Sociedad Química y Minera de Chile, S.A.*, No. 1:17-cr-00013, Deferred Prosecution Agreement (D.D.C. 13 Jan. 2017).

54 Exchange Act § 20(a), 15 U.S.C. § 17t(a).

55 See, e.g., *In re Mut. Funds Inv. Litig.*, 566 F.3d 111, 129–30 (4th Cir. 2009); *Laperriere v. Vesta Ins. Group*, 526 F.3d 715, 723–25 (11th Cir. 2008).

56 Exchange Act § 20(a), 15 U.S.C. § 17t(a).

57 *U.S. Sec. Exch. Comm'n v. Nature's Sunshine Prods., Inc.*, Civ. No. 2:09CV0672, Compl. (D. Utah 31 Jul. 2009).

58 Id.

© Law Business Research 2021

SEC Whistleblower Program 43.5

Over the past decade, directors have also faced increasing regulatory scrutiny as a result of the SEC Whistleblower Program, which provides monetary incentives for individuals to come forward and report possible violations of the federal securities laws to the SEC.[59] Since Congress established the Whistleblower Program pursuant to the Dodd-Frank Act, the SEC has imposed over US$2 billion in total monetary sanctions in enforcement matters brought with information from meritorious whistleblowers.[60]

Notably, under SEC Rule 21F-4, compliance personnel, auditors, directors and other employees can submit tips anonymously to the SEC and be eligible for a whistleblower award if (1) they have a reasonable basis to believe that disclosure is necessary to prevent conduct likely to cause 'substantial injury' to the financial interest or property of the entity or investors, (2) they have a reasonable basis to believe that the entity is engaging in 'conduct that will impede an investigation of the misconduct', or (3) at least 120 days have passed either since they properly disclosed the information internally, or since they obtained the information under circumstances indicating that the entity's officers already knew of the information. Under this authority, the SEC has issued three whistleblower awards to individuals with compliance or internal audit responsibilities.[61] Directors who fail to exercise their oversight responsibilities with respect to investigations may find themselves the target of SEC whistleblower complaints brought anonymously by compliance or internal audit personnel from within their corporations.

Duty of oversight in investigations 43.6

Directors' duty of oversight, and their obligation to act in good faith, are implicated at multiple stages of a corporate investigation – from the decision whether to initiate an investigation, to how to most appropriately design and implement such an investigation (e.g., choice of counsel); to the decision whether to self-disclose potential wrongdoing to regulators; to decisions authorising negotiation or settlement with regulators. At each stage, directors must ask appropriate questions, obtain sufficient information and engage in meaningful deliberation to satisfy themselves that the decision is in the best interests of the corporation. Increasingly, independent auditors threaten to initiate reporting procedures under Section 10A of the Exchange Act in the absence of an independent investigation into suspected wrongdoing.[62] In addition, direc-

59 SEC Whistleblower Program, Frequently Asked Questions, available at https://www.sec.gov/whistleblower/frequently-asked-questions#faq-1.

60 SEC Whistleblower Program, 2019 Annual Report, available at https://www.sec.gov/files/OW_2019AR_FINAL_1.pdf.

61 'SEC Awards $450,000 to Whistleblower', U.S. Securities and Exchange Commission (30 March 2020), available at https://www.sec.gov/news/press-release/2020-75.

62 Exchange Act § 10(A), 15 U.S.C. § 78j-1.

© Law Business Research 2021

tors must bear in mind that if the corporation is prosecuted for misconduct, prosecutors will consider the board's execution of its duty of oversight in sentencing the corporation.[63]

Moreover, directors play a central role in remediating issues identified during an investigation. Directors must oversee the process of enhancing or establishing internal controls for financial reporting, cybersecurity or other material aspects of the company's compliance infrastructure that are found lacking. This frequently requires directors to adapt to, and occasionally reassess, their view of company processes and the conduct of management based on facts developed during an investigation. At the same time, directors must interact with external auditors in connection with the issuance of an audit opinion and oversee a financial reporting process that contemplates such changes.

Director liability for breach of fiduciary duty frequently arises from the alleged failure of the board to respond to 'red flags' of corporate misconduct. When faced with actual knowledge or red flags of wrongdoing, directors must take good-faith steps to conduct reasonable inquiry to understand the cause and scope of the issue, and to implement appropriate remedial measures, as necessary. Directors may be subject to oversight liability because of inaction, wilful ignorance or failure to investigate and address possible misconduct in good faith.

As reflected in *Wells Fargo*, there are several ways in which a director may be considered to be on notice of possible corporate wrongdoing,[64] such as internal and external audit reports, whistleblower complaints, consumer complaints, news reports, regulatory investigations and related civil litigation claims. The case law emphasises the need for directors to respond to repeated signs of misconduct, since courts and regulators may interpret the absence of a response as a conscious disregard of the directors' duty of oversight. As the Delaware Court of Chancery explained:

> *a* Caremark *plaintiff can plead that "the directors were conscious of the fact that they were not doing their jobs," and that they ignored "red flags" indicating misconduct in defiance of their duties. A claim that an audit committee or board had notice of serious misconduct and simply failed to investigate . . . would survive a motion to dismiss, even if the committee or board was well constituted and was otherwise functioning.*[65]

63 See U.S. Fed. Sentencing Guidelines Manual § 8B2.1(b)(2)(A) ('The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program.').

64 *Wells Fargo*, 282 F. Supp. 3d at 1088, 1107–09.

65 *Shaev Profit Sharing Account v. Armstrong*, C.A. No. 1449-N, 2006 Del. Ch. LEXIS 33, at *16 (Del. Ch. 13 February 2006).

© Law Business Research 2021

Importantly, by virtue of the audit committee's oversight of accounting, internal controls and auditing matters, directors naturally receive information regarding the corporation's internal controls and compliance system that implicates their duty of oversight. This level of knowledge could subject directors to increased risk of regulatory scrutiny and private shareholder action if they fail to respond to internal control deficiencies and red flags of potential misconduct that are reported to them.

Strategic considerations for directors 43.7

While there is no effective one-size-fits-all approach to satisfaction of fiduciary duties, directors can take certain steps to meet the ongoing challenges and expectations of regulators and shareholders. Although such measures may not eliminate the risk of director liability, they will demonstrate directors' adherence to the core principles of their fiduciary duties.

- *Risk-based compliance framework*: Directors should require management to demonstrate that the company has adopted an effective risk-based compliance programme to identify high-risk compliance issues and prioritise resources accordingly.
- *Remaining informed*: Directors should implement a formal process that facilitates communications between the board and management regarding the compliance programme and business performance. Directors should remain informed about ongoing and acute risks, as well as about the broader business environment and industries in which the company is operating.
- *Independent investigations and compliance crises*: Directors should develop a crisis-management strategy and establish an investigative protocol before such measures are needed, including a process for the board to respond if an independent investigation is necessary. This may include proactive delegation of oversight responsibility to the company's audit committee or a special litigation or investigation committee. This also may include an annual presentation from management, including the legal and compliance functions, as to the company's readiness if a government inquiry, whistleblower complaint or other occurrence necessitates consideration of an independent investigation.
- *Training*: Directors should have sufficient training not only to be familiar with principles of corporate governance and the corporation's business, but also to provide directors a basis from which they can inquire about compliance risks and analyse responses consistent with their oversight responsibilities.
- *Overseeing the external auditor relationship*: The audit committee owns the relationship with the external auditor. Too often, directors limit their interaction with the external auditor to engagement of the auditor and a quarterly discussion in advance of the issuance of a filing. The better approach is for directors, particularly those on the audit committee, to establish a deeper relationship with external auditors that provides for a foundation of

See Chapter 46 on compliance

© Law Business Research 2021

trust and familiarity from which both parties can act when an unexpected problem arises.

- *Documenting directors' oversight work*: A documented approach to corporate governance and adherence to fiduciary duties can mitigate directors' risks in the event of litigation or an enforcement proceeding. Real-time documentation, including through minutes of audit committee or special investigative committee meetings, are critical evidence of directors' fulfilment of their oversight obligations in the context of a board committee's evaluation of issues involving investigations and compliance crises.

Effective board processes enable directors to carry out their responsibilities in accordance with applicable fiduciary duties and the expectations of regulators and the market. Adherence to sound principles of corporate governance protects directors and benefits the company in several forms, including through heightened investor confidence and corporate reputation; increased efficiency and avoidance of costly investigation due to early issue spotting and risk mitigation; and higher levels of customer and employee retention.

© Law Business Research 2021

44

Sanctions: The UK Perspective

Rita Mitchell, Simon Osborn-King and Yannis Yuen[1]

Introduction 44.1

Sanctions are restrictive measures aimed at achieving foreign policy or national security objectives. With the creation of the Office of Financial Sanctions Implementation (OFSI) in March 2016 and recent increases to the size and severity of penalties for sanctions breaches, sanctions enforcement is a growing area of economic crime enforcement in the United Kingdom. The United Kingdom has now implemented its autonomous sanctions regime following its exit from the European Union on 31 December 2020, which will likely lead to an increase in enforcement activity against corporates and individuals in the United Kingdom.

The United Kingdom currently implements and enforces sanctions implemented by the United Nations and its own domestic sanctions regime (which includes the sanctions imposed by the European Union which were retained in UK law after Brexit) against individuals, entities and jurisdictions. These include various restrictive measures, such as trade sanctions (e.g., arms embargoes and restrictions on dual-use items); economic or financial sanctions (e.g., asset freezes and restrictions on a variety of financial markets and services); and immigration sanctions (e.g., travel bans). While the Foreign and Commonwealth Office has overall responsibility for UK government policy on international sanctions, trade sanctions are generally monitored and enforced by the Department for International Trade (DIT) (acting through the UK Export Control Joint Unit (ECJU)) or Her Majesty's Revenue and Customs (HMRC). Financial sanctions are administered and enforced by OFSI (with

1 Rita Mitchell and Simon Osborn-King are partners, and Yannis Yuen is an associate, at Willkie Farr & Gallagher LLP.

© Law Business Research 2021

support from the National Crime Agency (NCA)), and immigration sanctions by the Home Office. In addition to civil enforcement, criminal prosecution of sanctions violations may be pursued by HMRC or the Serious Fraud Office (SFO) upon referral by OFSI, or by the Crown Prosecution Service (CPS) for breaches of trade sanctions. Regulators, such as the Financial Conduct Authority (FCA), also ensure that regulated firms have adequate systems and controls in place to enable them to meet their sanctions obligations.

In this chapter, we set out an overview of the UK sanctions framework, and consider how investigations may arise and what are best practices when initiating or responding to investigations.

44.2 Overview of the UK sanctions regime

44.2.1 Statutes and official guidance

The United Kingdom has historically followed the United Nations and European Union in applying sanctions. EU sanctions are implemented through regulations with direct legal effect in Member States,[2] with individual Member States being responsible for enforcement of EU sanctions.[3] Post-Brexit, EU sanctions no longer apply in the United Kingdom, but it has implemented EU sanctions into national law through secondary legislation. Existing EU sanctions regimes are addressed under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA), which provides the legal basis for the United Kingdom to impose, update and lift sanctions following Brexit. The United Kingdom also has its own terrorist sanctions regime. Entities in the regulated sector are subject to the Anti-Terrorism, Crime and Security Act 2001, the Counter-Terrorism Act 2008 and the Terrorist Asset-Freezing etc. Act 2010. OFSI has issued guidance regarding its approach to financial sanctions under SAMLA,[4] as well as an enforcement guide that summarises its approach to compliance and enforcement, including the imposition of penalties.[5] Broadly speaking, the guidance issued by OFSI shows that it has high expectations with regard to sanctions compliance. In particular, licensing grounds are interpreted narrowly, and it is clear that general and specific reporting obligations are a key aspect of the United Kingdom's sanctions enforcement apparatus. When assessing sanctions violations, OFSI will treat each breach on its own merits based on

2 See, e.g., Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No. 329/2007 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R1509-20200603).

3 See, e.g., The Democratic People's Republic of Korea (European Union Financial Sanctions) Regulations 2017 (https://www.legislation.gov.uk/uksi/2017/218).

4 OFSI Financial Sanctions Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf.

5 OFSI Enforcement Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf).

© Law Business Research 2021

a number of aggravating and mitigating factors, and in particular, will place substantial value on co-operation and timely voluntary disclosure.

Persons to whom sanctions apply 44.2.2

UK nationals and entities established under UK law, and their overseas branches, must comply with UK sanctions regardless of where they are located or their activities take place. UK financial sanctions also apply to any individual or entity located within the United Kingdom or that carries out activities there. In its published guidance, OFSI provides a number of non-exhaustive examples of how a UK nexus might arise, including a UK company working overseas, transactions using clearing services in the United Kingdom, actions by a local subsidiary of a UK company, or actions taking place overseas but directed from within the United Kingdom.[6]

Restrictive sanctions measures apply to named individuals, entities, groups, sectors or countries. OFSI maintains a list of individuals and entities subject to financial sanctions to help individuals and businesses comply with those sanctions. Consistent with EU guidance, OFSI considers that if a designated person owns more than 50 per cent of, or otherwise controls, an entity (directly or indirectly),[7] financial sanctions will apply to that entity as well.

Unlike the situation in the United States, the UK sanctions regime does not include secondary sanctions. Council Regulation (EC) No. 2271/96, known as the 'Blocking Statute', enshrined into law in the United Kingdom,[8] prohibits UK residents and companies from complying with certain extraterritorial legislation, specifically in relation to US sanctions on Cuba and Iran, unless they are exceptionally authorised to do so by the Secretary of State. The Blocking Statute also allows UK residents and companies to recover damages arising from such legislation from the persons or entities causing them, and prevents any foreign court rulings based on the blocked legislation from having effect in the United Kingdom.[9]

6 OFSI Enforcement Guidance at paragraph 3.7 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf).

7 OFSI Financial Sanctions Guidance at section 4 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf).

8 Via The Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2020 (https://www.legislation.gov.uk/uksi/2020/1660/contents/made).

9 Council Regulation (EC) No. 2271/96 (https://www.legislation.gov.uk/eur/1996/2271/contents), Articles 4, 5 and 6, as amended by The Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2020.

© Law Business Research 2021

44.2.3 Exemptions and licensing

The UK sanctions regime provides for certain exceptions from the restrictive measures imposed under sanctions legislation in the form of exemptions or licences. With respect to exemptions, in certain limited situations and conditions as set out in the legislation, particular activities are automatically exempt, meaning that parties may engage in the activity without a licence or authorisation. Alternatively, for activities that would otherwise be prohibited, parties may apply for a licence. OFSI oversees applications for licences in relation to financial sanctions, and DIT for trade sanctions. OFSI will only grant a licence where it falls within the specific grounds identified in the underlying legislation. Generally these cover areas such as basic needs, legal fees and disbursements, fees or charges relating to frozen accounts and other economic resources, payment of court judgments or arbitration decisions against a designated person, satisfaction of contractual obligations, and other extraordinary expenses.[10]

OFSI may also grant licences in accordance with the United Kingdom's domestic terrorist sanctions regimes (without the need for specific licensing grounds), and can issue licences specific to individuals or generally applicable to all persons designated under particular domestic terror sanctions regimes.[11] As of August 2021, there is only one active general licence under the United Kingdom's domestic terrorist sanctions regime.[12] General licences can be used without making an application to OFSI, but there is an obligation to report their use without delay.[13]

Where an individual or entity seeks to import or export goods restricted by sanctions, such as dual-use goods (items with both a military and civilian use), a licence may be required by the ECJU alongside one from OFSI.

44.2.4 Key jurisdictions

While a number of jurisdictions are sanctioned by the United Kingdom, three are particularly significant: Iran, North Korea and Russia/Ukraine.

10 OFSI Financial Sanctions Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf) at para. 6.5.

11 For example, see the Terrorist Asset-Freezing etc. Act 2010 (https://www.legislation.gov.uk/ukpga/ 2010/38/contents), s.17.

12 General Licence INT/2020/G1 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/988364/General_Licence_-_INT2020G1_-_As_amended.pdf).

13 OFSI Financial Sanctions Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf) at para. 6.8.1.

© Law Business Research 2021

Iran 44.2.4.1

On 16 January 2016, the European Union lifted all of its economic and financial sanctions in connection with the Iranian nuclear programme pursuant to the Joint Comprehensive Plan of Action (JCPOA) between the E3/EU+3 (France, Germany and the United Kingdom, plus Russia, China and the United States) and Iran.

There are, however, certain measures and restrictions relating to proliferation that remain in place for the United Kingdom, including an arms embargo, restrictive measures relating to missile technology, restrictions on nuclear-related transfers and activities, and an authorisation regime for certain metals and software.[14]

Separate restrictive measures independent of the JCPOA also still apply. These were historically imposed by the European Union in relation to serious human rights violations in Iran, and include asset freezes, travel bans and a ban of exports to Iran of equipment that may be used for internal repression or equipment for monitoring telecommunications. Following the withdrawal of the United States from the JCPOA and the re-implementation of US secondary sanctions on Iran, the European Union amended the Blocking Statute to include the list of extraterritorial US sanctions on Iran. This change was retained by the United Kingdom following Brexit.[15]

North Korea 44.2.4.2

North Korea is subject to a number of counter-proliferation measures aimed at preventing individuals and entities from obtaining funds, goods or services that could contribute to North Korea's nuclear proliferation programme. These measures are wide-ranging and include, for example, asset freezes, travel bans, sectoral financial sanctions, restrictions on particular services and financial assistance, prohibitions on the export and procurement of arms and on the export of luxury or dual-use goods.[16]

Russia/Ukraine 44.2.4.3

The United Kingdom has retained numerous economic, trade and financial restrictive measures on Russia originally imposed by the European Union in response to the annexation of Crimea and Sevastopol, and actions that

14 'UK sanctions relating to Iran (nuclear weapons)' (https://www.gov.uk/government/collections/uk-sanctions-on-iran-relating-to-nuclear-weapons).

15 See Council Regulation (EC) No. 2271/96 (https://www.legislation.gov.uk/eur/1996/2271/contents), as amended by The Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2020).

16 'UK sanctions relating to the Democratic People's Republic of Korea' (https://www.gov.uk/government/collections/uk-sanctions-on-the-democratic-peoples-republic-of-korea).

© Law Business Research 2021

undermine or threaten the territorial sovereignty and independence of Ukraine. Alongside asset freezes and travel bans, it is also prohibited to:

- import or export arms and related material to or from Russia;
- sell, supply, transfer or export dual-use goods and technology for military use in Russia or to specific designated persons;
- provide loans or credit with a maturity exceeding 30 days to specific designated persons;
- export certain equipment, or provide technical and financial assistance or other services, in connection with the export, sale or transfer of such equipment without prior authorisation; and
- provide services for particular forms of oil exploration and production.[17]

44.3 Offences and penalties

The various regulations for each sanctions regime set out prohibited conduct. Offences typically arise from dealing with funds or economic resources belonging to, owned, controlled or held by a designated person without a licence while knowing or suspecting that the transaction is prohibited. This can include making funds or economic resources available to a designated person, dealing with funds or economic resources that must be frozen, circumventing an asset freeze or breaching licensing conditions.[18] For example, OFSI imposed a monetary penalty on Telia Carrier UK Limited for indirectly facilitating international phone calls to a designated Syrian entity, which counted as making funds and economic resources indirectly available to it.[19] The sanctions regime allows criminal or civil cases to be brought for sanctions violations depending on the facts and the conduct in question.

44.3.1 Criminal penalties

Criminal prosecutions can only be brought if there is sufficient evidence to provide a realistic prospect of conviction, and the prosecution is in the public interest.[20] Criminal prosecutions of corporates for sanctions breaches are, however, unlikely, not least due to the difficulty of establishing corporate criminal liability in the United Kingdom. Civil breaches are enforced by OFSI, and criminal breaches are enforced by the SFO, HMRC and the CPS.

The penalties for breaches of sanctions in the United Kingdom are set out in the relevant statutory instruments. Criminal violations typically include

17 'UK sanctions relating to Russia' (https://www.gov.uk/government/collections/uk-sanctions-on-russia).

18 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf.

19 'Imposition of Monetary Penalty – Telia Carrier UK Limited' 9 September 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/842548/Telia_monetary_penalty.pdf).

20 The Code for Crown Prosecutors (https://www.cps.gov.uk/publication/code-crown-prosecutors).

© Law Business Research 2021

unlimited criminal fines, and up to seven years' imprisonment for sanctions violations, as set by the Policing and Crime Act 2017 (PACA).[21]

Criminal breaches of sanctions may also have money-laundering implications. The Proceeds of Crime Act 2002 (POCA), which broadly prohibits the handling of criminal property (defined as any benefit resulting from criminal conduct) has extraterritorial application, and even property resulting from criminal conduct that occurs abroad may be caught by POCA. For example, any payments received in the United Kingdom as part of a transaction that would constitute a sanctions offence would fall within the definition of 'criminal property' in POCA. The subsequent handling of those funds with the knowledge that they were criminal property would then constitute a money laundering offence. The maximum penalties for breaching POCA include an unlimited fine and up to 14 years' imprisonment.[22]

The Serious Crime Act 2007 also allows a High Court judge to impose a serious crime prevention order on an individual or entity that has been involved in a serious crime, including breaches of financial sanctions.

Civil penalties 44.3.2

For breaches of sanctions that satisfy the civil standard of proof, OFSI may also impose monetary penalties of up to £1 million or 50 per cent of the value of the breach, whichever is higher.[23]

Sanctions investigations 44.4

Sanctions investigations can arise in a number of ways. Internally, a company may become aware of a whistleblower report, red flags arising from automated compliance systems and controls, or findings from internal or external audits. A company may also receive notification from a bank of a blocked payment. UK authorities also increasingly commence investigations based on suspicious activity reports (SARs) filed with the NCA, voluntary self-reports by the company itself,[24] or reports from other individuals, entities or enforcement agencies. There is no general notification requirement to inform a suspect that they are under investigation. As a result, a suspect may not become aware of

21 This was an increase on the previous maximum penalty of two years. See the European Communities Act 1972 (https://www.legislation.gov.uk/ukpga/1972/68/contents), Schedule 2, para. 1(1)(d).

22 Proceeds of Crime Act 2002 (https://www.legislation.gov.uk/ukpga/2002/29/contents), s.334.

23 Policing and Crime Act 2017 (https://www.legislation.gov.uk/ukpga/2017/3/contents/enacted), s.146(3).

24 For example, under the Terrorist Asset Freezing etc. Act 2010, certain institutions have an affirmative reporting obligation to the Treasury where they have knowledge or reasonable cause to suspect that someone is a designated person or has committed an offence involving certain prohibitions in relation to designated persons. See Terrorist Asset Freezing etc. Act 2010, s.19.

© Law Business Research 2021

an investigation without an overt act such as the service of production orders, the arrest of one or more individuals, an asset freeze or the execution of a search warrant.

OFSI has broad investigative powers to require any person located or resident in the United Kingdom to produce or provide information or documents to allow it to establish the extent of funds and economic resources linked to a designated person, obtain information concerning the disposal or transfer of such funds or economic resources, monitor compliance with or evasion of sanctions, or obtain evidence of the commission of an offence. Failure to comply with such requests without a reasonable excuse or obstructing OFSI in its investigation is a criminal offence.

Although OFSI is the primary agency responsible for sanctions, it may also refer a matter to other government agencies, such as the SFO or HMRC, both of which may also potentially pursue a criminal prosecution. The SFO and HMRC also have broad powers to request or require information,[25] and HMRC may also make arrests.

OFSI also works closely with the NCA and may receive information on suspected breaches from the NCA's International Corruption Unit.[26] The NCA typically refers cases for prosecution to the CPS, which may also prosecute breaches of trade sanctions pursuant to the Crown and Excise Management Act 1979.

Regulated entities could also be subject to enforcement action by the FCA for failure to maintain effective systems and controls to address the risk of sanctions violations,[27] effective systems and controls relating to compliance, financial crime and money laundering,[28] and adequate policies and procedures to counter the risk of financial crime.[29]

See Chapter 11 on production of information

The FCA may issue notices to authorised persons requiring them to produce specified documents or information.[30] The FCA may choose to request that documents be provided voluntarily, in the first instance. Although regulated entities need not comply with voluntary requests, they must deal with

25 For example, see Criminal Justice Act 1987, s.2.

26 See https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion.

27 FCA's Principles for Business (https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html), Principle 3.

28 FCA's Senior Management Arrangements, Systems and Controls Sourcebook (https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html), Rule 3.2.6.

29 ibid. (https://www.handbook.fca.org.uk/handbook/SYSC/6/1.html), Rule 6.1.1.

30 Financial Services and Markets Act (FSMA) (https://www.legislation.gov.uk/ukpga/2000/8/section/165), s.165.

© Law Business Research 2021

the FCA 'in an open and cooperative way' and 'disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice'.[31]

Once the FCA has formally commenced an investigation, it may require the subject of the investigation (or a person connected to the subject) to produce documents, attend interviews and answer questions, or otherwise provide information required by the investigator, where the documents or information sought are reasonably relevant to the investigation.[32] Furthermore, the FCA may seek answers and documents from persons who are not actually subject to investigation or connected to a person subject to investigation, where 'necessary or expedient for the purposes of the investigation'.[33]

Best practices in investigations 44.5

Factors to consider 44.5.1

The creation of OFSI and recent enforcement activity in the United Kingdom demonstrates that sanctions enforcement and investigations is a priority area in the prosecution of economic crime. There is also a pronounced emphasis by UK enforcement authorities on voluntary disclosure and ongoing co-operation, with the FCA noting that 'the requirement on firms to deal with their regulator openly and cooperatively is a central part of the Authority's regulatory regime',[34] and the SFO similarly stating that 'co-operation will be a relevant consideration in the SFO's charging decisions'.[35] For that reason, it will be important for a company to move quickly, while balancing speed against substance to ensure that it understands the nature of the alleged violation and the risks it presents. Issues for consideration may include:

- to whom and when to give notice of the issue or investigation;
- identifying who was involved in or responsible for the alleged breach;
- preserving relevant information regarding the alleged breach and the company's response;
- conducting an internal investigation into the alleged breach and potentially any related transactions or departments;
- remediation;
- dealing with auditors;
- disciplinary action; and
- external communication strategy.

31 FCA's Principles for Business (https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html), Principle 11.

32 FSMA (https://www.legislation.gov.uk/ukpga/2000/8/section/171), s.171.

33 ibid. (https://www.legislation.gov.uk/ukpga/2000/8/section/172), s.172.

34 Final Notice – Tullett Prebon (Europe) Limited, 11 October 2019 (https://www.fca.org.uk/publication/final-notices/tullett-prebon-europe-limited-2019.pdf), para. 6.45.

35 SFO Corporate Co-operation Guidance (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/corporate-co-operation-guidance/).

© Law Business Research 2021

44.5.2 Co-operation

Co-operation with a UK authority may be mandatory where, for example, the authority has exercised its investigative powers and has issued notices requiring the provision of information or production of documents.

Where co-operation is voluntary, an individual or entity under investigation may still wish to co-operate fully with the UK authority for various reasons. Co-operation may result in a more positive outcome, such as a civil rather than criminal penalty, or conclusion of a criminal investigation by way of a deferred prosecution agreement (DPA). It may also result in a faster resolution of the matter, which may reduce legal fees and save valuable management time.

Other tangible benefits to co-operation include being able to work with the authority in shaping any public announcements as well as internal communications associated with the investigation, or the ability to gently influence an investigation through increased contact and rapport with the relevant authorities.

44.5.2.1 Self-reporting

Considerations

As of April 2021, OFSI has updated its enforcement guidance to state that breaches of financial sanctions 'must' be reported to it (a change from the previous 'should').[36] Specific reporting obligations also apply to certain 'relevant firms'. Given the potential benefits, self-reporting is an important consideration when faced with a potential sanctions violation.

When assessing the seriousness of a case, authorities will take self-reporting into account, and may consequently offer a more lenient outcome.[37] Any delay in self-reporting risks the authorities discovering the violation through other sources. This may prevent a person from qualifying for the penalty reduction given by OFSI for prompt and complete voluntary self-disclosures, although OFSI does consider it reasonable for a person to take 'some time to assess the nature and extent of the breach, or seek legal advice' as long as this does not delay an effective response to the breach.[38] By way of example, in its investigation of Standard Chartered Bank, OFSI allowed the bank first to disclose the

36 OFSI Enforcement Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf) at para. 3.27.

37 For example, Standard Chartered Bank was able to secure a 30 per cent reduction for its voluntary self-disclosure (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf).

38 OFSI Enforcement Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf), para. 3.32.

© Law Business Research 2021

suspected breaches, followed by interim updates of its internal investigation and a final report at the end of the bank's internal investigation.[39]

However, self-reporting is not without risk. A self-report, especially if incomplete, may lead authorities to conduct further investigations of the company's activities, which could be expensive and lengthy, and expose new issues. There is also no guarantee of a lenient approach, especially if the violations were carried out knowingly, were egregious, or were avoidable with an effective compliance programme. It is best practice, therefore, to consider a self-report with the guidance of experienced legal counsel and after a preliminary investigation of the facts.

See Chapter 3 on self-reporting

Reporting obligations

All individuals and entities subject to UK sanctions must report any breaches of financial sanctions to OFSI.

Specific reporting obligations also apply to the following 'relevant firms':

- persons with permission to carry out regulated activities;[40]
- businesses that transmit money by any means, operate a currency exchange office or cash cheques payable to customers;
- a firm or sole practitioner that is a statutory auditor or local auditor;
- a firm or sole practitioner that provides by way of business accountancy services, legal or notarial services, advice about tax affairs or certain trust or company services;
- a firm or sole practitioner that carries out, or whose employees carry out, estate agency work;
- the holder of a casino operating licence; or
- a person engaged in the business of making, supplying, selling or exchanging articles made from gold, silver, platinum, palladium or precious stones or pearls.[41]

Relevant firms must report to OFSI if they have knowledge or reasonable cause to suspect that a third party is a designated person or has committed an offence under the regulations. If a relevant firm knows or has reasonable cause to suspect that a third party is a designated person, and is also a customer of the relevant firm, then the relevant firm must also state the nature and amount or quantity of any funds or economic resources held for that customer.

Additional reporting to other authorities may be necessary, such as to the FCA or the NCA. Specific reporting obligations may also arise under section 19 of the Terrorism Act 2000 for any act known or suspected to be

39 'Imposition of Monetary Penalty – Standard Chartered Bank', 18 February 2020 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf).

40 Under FSMA (https://www.legislation.gov.uk/ukpga/2000/8/contents), Part 4A.

41 Definitions of each of these businesses and professions can be found in the relevant UK regulation for each sanctions regime.

© Law Business Research 2021

linked to terrorist financing, as well as under the statutory scheme for each sanctions regime. Where the violation also involves complex fraud or international bribery and corruption, a person may also consider self-reporting to the SFO.

44.5.3 Settlement

OFSI has discretion in how it responds to breaches of financial sanctions. For example, it may simply require a company to provide additional information about its compliance practices. It may also impose monetary penalties or refer a matter to other regulators or criminal authorities for prosecution.[42]

Criminal breaches of sanctions are eligible for DPAs with the CPS and SFO, allowing an organisation to make reparations for its behaviour without many of the consequences of a conviction. A DPA allows organisations that have co-operated with authorities during an investigation to have the proceedings against them suspended for a set period. The DPA will contain provisions that address the payment of a monetary penalty, compensation, or both; the implementation of a compliance programme; and an agreement for future co-operation with the relevant authority. Upon expiry of the DPA, assuming all obligations are fully met, the prosecution will be discontinued. A code of practice setting out guidance in relation to DPAs has been jointly issued by the CPS and SFO.[43] Since the United Kingdom introduced its DPA programme in 2014,[44] the SFO had entered into 12 DPAs as of August 2021.

For breaches that only satisfy the civil standard and would incur a monetary penalty from OFSI, it is also possible to minimise penalties by making a voluntary self-report in the first instance, making representations during the penalty decision process and appealing OFSI's penalty recommendation through ministerial review.

In reaching a penalty decision, OFSI will assess the seriousness of a case based on a number of mitigating and aggravating factors, including but not limited to:

- whether funds or economic resources were provided directly to a designated person;
- whether there was an intentional circumvention of sanctions;
- the value of the breach;
- knowledge of sanctions and compliance systems (although ignorance is no defence);

42 OFSI Enforcement Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf), para. 3.2.

43 'Deferred Prosecution Agreements Code of Practice', 11 February 2014 (https://www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf).

44 Crime and Courts Act 2013 (https://www.legislation.gov.uk/ukpga/2013/22/contents/enacted), Schedule 17.

© Law Business Research 2021

- the behaviour at issue, including, for example, whether the breach was deliberate or negligent, or any management involvement in the breach;
- repeated, persistent or extended breaches; and
- reporting of breaches to OFSI, including whether the disclosure was voluntary, materially complete and made in good faith.

Where OFSI concludes that the threshold for imposing a civil penalty has been met, it will begin with the statutory maximum penalty it can impose, which will be the greater of £1 million or 50 per cent of the value of the breach. OFSI then decides what level of penalty, between zero and the maximum, is reasonable and proportionate, based on aggravating and mitigating factors. Up to a 50 per cent reduction in the final penalty is available to persons who provide a prompt and complete voluntary disclosure. This applies to cases assessed as 'serious', while a 30 per cent reduction is available for cases assessed to be 'most serious'. OFSI then produces a penalty recommendation, in respect of which the company can make representations.

Section 147 of the Policing and Crime Act 2017 also confers a right on any subject of OFSI enforcement action to appeal the fine by requesting a ministerial review of the penalty recommendation. Some OFSI enforcement decisions indicate that invoking this right may result in substantially reduced penalties.

Trends and key issues 44.6

Recent enforcement activity 44.6.1

As at August 2021, OFSI had imposed five monetary penalties for breaches of financial sanctions since it was first given powers to do so in April 2017. These fines have varied in size, and only two have exceeded £100,000.[45] Standard Chartered Bank (SCB) was fined £20.47 million in February 2020 for violating sanctions targeting Russia/Ukraine, making it the first fine in the United Kingdom relating to the EU Ukraine (Sovereignty and Territorial Integrity) sanctions regime.[46] Based on these violations, OFSI reached a penalty recommendation of £31.5 million. However, this was appealed by SCB through the ministerial review process and the penalty was subsequently reduced. Telia Carrier UK Limited likewise successfully appealed its original penalty recommendation of £300,000 through ministerial review, reducing it by roughly half in relation to sanctions violations targeting Syria.[47] Most recently in August 2021, TransferGo was fined £50,000 for transferring funds to accounts held

45 'Enforcement of financial sanctions' (https://www.gov.uk/government/collections/enforcement-of-financial-sanctions).

46 'Imposition of Monetary Penalty – Standard Chartered Bank', 18 February 2020 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf).

47 'Imposition of Monetary Penalty – Telia Carrier UK Limited', 9 September 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/842548/Telia_monetary_penalty.pdf).

© Law Business Research 2021

with the Russian National Commercial Bank (RNCB), an entity subject to an asset freeze.[48] Although TransferGo's fine is substantially lower than those levied on SCB or Telia, the total value of transactions in breach of sanctions was just £7,764.77. The size of the penalty therefore demonstrates that the financial value of relevant transactions is only one component in OFSI's overall assessment of sanctions breaches.[49] Furthermore, notwithstanding later co-operation with OFSI, because TransferGo did not voluntarily disclose the transactions, it was not eligible for voluntary disclosure credit. TransferGo's attempt to appeal the fine was unsuccessful.

In April 2019, the FCA fined SCB £102.2 million for anti-money laundering (AML) breaches connected in part to violations of US sanctions, based on findings of shortcomings in SCB's internal assessments of the adequacy of its AML controls, its approach to identifying and mitigating money laundering risks and its escalation of money laundering risk.[50] This matter serves as a reminder that even if a particular transaction does not breach UK or EU sanctions, it may still face collateral enforcement action in the United Kingdom for compliance programme failures.

44.6.2 Potential pitfalls

While OFSI's enforcement activity still pales in comparison to its US counterpart – the US Department of the Treasury's Office of Foreign Assets Control – which issued US$1.29 billion of monetary penalties in 2019[51] (although this figure decreased to US$24.6 million in 2020),[52] the current trend of OFSI's fines suggests that enforcement activity will only intensify. As an enforcement agency, OFSI continues to mature, and it is likely that OFSI has numerous investigations in the pipeline.

Brexit may also lead to a divergence between the EU and UK sanctions regimes. For example, EU sanctions provide an exemption to restrictions on particular financial activities in Russia for EU-based subsidiaries of designated entities. After 31 December 2020, any UK-based subsidiaries of designated

48 'Imposition of Monetary Penalty – TransferGo Limited', 25 June 2021 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008859/050821_-_TransferGo_Penalty_Report.pdf).

49 OFSI Enforcement Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708991/Monetary_Penalties_Guidance_web.pdf) at para. 3.17.

50 'Decision Notice – Standard Chartered Bank', 5 February 2019 (https://www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf).

51 2019 Enforcement Information – US Department of the Treasury (https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information).

52 2020 Enforcement Information – US Department of the Treasury (https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2020-enforcement-information)

© Law Business Research 2021

entities under this sanctions regime will only be exempt from the UK equivalent of this restriction, and *vice versa*. The United Kingdom has also expanded the prohibition of 'financial assistance' relating to the supply of certain goods. While the Court of Justice of the European Union has held that 'financial assistance' does not include payment processing,[53] the UK equivalent of this sanctions regime refers to the provision of 'financial services' instead, which includes payment processing.[54]

Additionally, OFSI has issued post-Brexit guidance extending the scope of financial sanctions to entities owned or controlled, directly or indirectly, by a designated person.[55] Substantial changes to the designation process are also in train. SAMLA brings with it a lower threshold for the imposition of sanctions as compared with the EU regime, requiring only that it be 'appropriate' to designate a person, rather than having to satisfy the 'necessity test' under EU law.[56] It also provides for the designation of persons by description,[57] which does not currently feature in the EU sanctions regime, and which may result in identification challenges for sanctions screening and compliance processes in future. Lastly, instead of seeking redress in the EU courts, a person designated under the United Kingdom's autonomous sanctions regime post-Brexit may seek variation or revocation of the designation by the Secretary of State or HM Treasury.[58]

SAMLA also introduces US-style general licence exemptions (separate from OFSI's existing powers to issue general licences around the United Kingdom's domestic terror sanctions regime), which allow a person to undertake acts that would otherwise be prohibited without the need to apply for a specific licence.[59]

Further divergence from the European Union can be seen in the United Kingdom's enactment of the Global Anti-Corruption Sanctions Regulations 2021 on 26 April 2021, which specifically target individuals involved in serious corruption, and authorise asset freezes and travel bans on individuals and

53 *PJSC Rosneft Oil Company v. Her Majesty's Treasury and Others* (Case C-72/15) (http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0072&lang1=en&type=TXT&ancre=).

54 The Russia (Sanctions) (EU Exit) Regulations 2019 (https://www.legislation.gov.uk/uksi/2019/855/contents/made) ss.28, 37, 44, and 52. See also Russia Guidance – Guidance for the financial and investment restrictions in Russia (Sanctions) (EU Exit) Regulations 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892741/OFSI_-_Russia_guidance_-_June_2020.pdf) (noting that financial services includes payment processing).

55 OFSI Financial Sanctions Guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf), s.4.

56 Sanctions and Anti-Money Laundering Act 2018 (https://www.legislation.gov.uk/ukpga/2018/13/contents), s.11.

57 ibid., s.12.

58 ibid., s.23.

59 ibid., s.15.

© Law Business Research 2021

asset freezes on entities.[60] This is in addition to the Global Human Rights Sanctions Regulations 2020,[61] representing the United Kingdom's first use of Magnitsky-style sanctions and preceding the European Union's own set of human rights sanctions legislation by four months.[62] These important developments demonstrate that the United Kingdom is still able and willing to take the lead on sanctions enforcement, instead of reacting and following in European footsteps.

In light of the above, individuals and entities are well advised to stay informed of any developments in this sphere, and to ensure that any sanctions compliance programme is sufficiently robust and agile enough to adapt to the shifting landscape of the United Kingdom's autonomous sanctions regime.

60 The Global Anti-Corruption Sanctions Regulations 2021 (https://www.legislation.gov.uk/uksi/2021/488/contents/made).

61 The Global Human Rights Sanctions Regulations 2020 (https://www.legislation.gov.uk/uksi/2020/680/contents/made).

62 Council Regulation (EU) 2020/1998 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02020R1998-20210322).

© Law Business Research 2021

45

Sanctions: The US Perspective

David Mortlock, Britt Mosman, Nikki Cronin and Ahmad El-Gamal[1]

Overview of the US sanctions regime 45.1

The United States imposes economic and trade sanctions on individuals, entities and jurisdictions based on US foreign policy and national security goals. These measures are administered and enforced primarily by the US Department of the Treasury's Office of Foreign Assets Control (OFAC), through a combination of statutes, regulations, executive orders and interpretive guidance. OFAC's regulations are strict liability, meaning that OFAC need not prove fault or intent to enter an enforcement action and issue a civil penalty. Additionally, if a party wilfully violates US sanctions laws, the Department of Justice (DOJ) and the US Attorney may pursue criminal investigations and enforcement actions. Other regulators, such as the Financial Crimes Enforcement Network and the New York Department of Financial Services, may also play a role in enforcing US sanctions regulations, imposing additional penalties for failures to maintain specific controls to help ensure compliance with OFAC administered regulations. Both federal and state regulators may pursue enforcement actions for the same conduct simultaneously, potentially leading to multiple related investigations by several entities.

The United States maintains comprehensive sanctions programmes, also called embargoes, generally prohibiting activity involving Cuba, Iran, North Korea, Syria and the Crimea region of Ukraine. In addition to comprehensive sanctions, OFAC implements targeted sanctions on specific individuals and entities (persons) under one or more of its sanctions programmes targeting various activities, such as narcotics trafficking, terrorism, proliferation activities

1 David Mortlock and Britt Mosman are partners, and Nikki Cronin and Ahmad El-Gamal are associates, at Willkie Farr & Gallagher LLP.

© Law Business Research 2021

involving nuclear or other weapons of mass destruction, or human rights violations. Both direct and indirect activities involving governments or persons subject to targeted sanctions can give rise to violations of US sanctions laws.

45.1.1 Statutes and official guidance

The United States maintains several sanctions regimes, each with its own restrictions and regulations. In addition to the country-specific sanctions programmes, such as the Iranian Transactions and Sanctions Regulations (ITSR), which primarily govern US sanctions on Iran, OFAC can also sanction persons under several targeted sanctions programmes, such as the Foreign Narcotics Kingpin Act or the Global Magnitsky Act. Pursuant to these sanctions programmes, persons designated by the State or Treasury Departments will be added to OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List). US persons are generally prohibited from engaging in any transactions, directly or indirectly, involving persons on OFAC's SDN List, as well as any entity of which 50 per cent or more is owned by one or more persons on the SDN List, unless authorised by OFAC or exempt. In addition, the sanctions programmes administered by OFAC also generally prohibit US persons from 'facilitating' actions of non-US persons, which, although completely legal for a non-US person, could not be directly performed by US persons owing to sanctions restrictions.

OFAC also imposes sanctions on persons in certain sectors of Russia's economy that are listed in OFAC's Sectoral Sanctions Identifications List (SSI List). Listed persons operating in identified sectors of the Russian economy, such as financial services, energy and defence, will be added to the SSI List under one of the four Directives described in Executive Order 13662.[2] Each Directive places specific prohibitions, requirements and restrictions on transactions by US persons with those listed persons.

OFAC maintains an updated list of US sanctions programmes and country information on its website[3] and a list of compiled frequently asked questions that provide a wide range of details and guidance on topics, including OFAC's interpretation of newly issued sanctions regulations, enforcement practices specific to certain sanctions programmes and the implementation of authorisations provided in general licences.[4] OFAC also regularly releases separate guidance documents that advise companies of specific risk factors for certain industries and suggest best practices for designing appropriate sanctions compliance programmes.

2 Exec. Order No. 13662, 79 Fed. Reg. 16169-71 (24 March 2014).

3 Available at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.

4 The US Department of the Treasury's Office of Foreign Assets Control (OFAC) FAQs are available at https://home.treasury.gov/policy-issues/financial-sanctions/faqs.

© Law Business Research 2021

OFAC's enforcement authority and procedures are set forth in OFAC's Economic Sanctions and Enforcement Guidelines at 31 CFR Part 501 Appendix A. The guidelines establish, among other things, the potential outcomes of an investigation or enforcement action and the method and relevant factors for calculating the base penalty amount of an apparent sanctions violation.

Persons to whom sanctions apply 45.1.2

US sanctions generally restrict activities within the jurisdiction of the United States and by US persons, generally defined as any US citizen, permanent resident alien, entity organised under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.[5] For Iran and Cuba, the prohibitions also extend to any entity owned or controlled by a US person.

The US government may also impose sanctions against non-US persons for certain activity, even with no nexus to the United States. 'Secondary sanctions' authorise OFAC or the State Department to impose sanctions against non-US persons for certain specified activity with Iran, Russia, North Korea and Syria. These are intended to discourage non-US persons from engaging in the specified activity and can result in sanctions against the foreign company itself. For example, when the United States reimposed secondary sanctions for certain activity involving specified sectors of the Iranian economy following the US withdrawal from the Joint Comprehensive Plan of Action (JCPOA), non-US persons became exposed to secondary sanctions for engaging in certain significant activity involving Iran's automotive, shipping, shipbuilding or energy sectors, or involving Iranian SDNs.[6]

Licensing 45.1.3

OFAC may issue a general licence or a specific licence to authorise certain activity that would otherwise be prohibited by sanctions.

A general licence is available to any person engaging in activity that fits the criteria set forth in the licence. Each general licence relates to a particular sanctions programme and generally offers broad authorisations covering certain categories of transactions. For example, a general licence is typically available to authorise the export of food, medicine and medical devices to countries subject to a comprehensive embargo. In addition to the general licence for

5 See OFAC FAQ #11.

6 OFAC will consider the totality of the circumstances when determining whether a transaction is significant, using seven factors: (1) the size, number and frequency of the transaction(s); (2) the nature of the transaction(s); (3) the level of awareness of management and whether the transaction(s) are part of a pattern of conduct; (4) the nexus between the transaction(s) and a blocked person; (5) the impact of the transaction(s) on statutory objectives; (6) whether the transaction(s) involve deceptive practices; and (7) such other factors that the Secretary of the Treasury deems relevant case by case. OFAC FAQ #545.

© Law Business Research 2021

the export of food, medicine and medical devices, most sanctions programmes also include general licences permitting certain transactions with respect to official business of the US federal government or international organisations such as the United Nations, certain transactions related to the transmission of telecommunications and the services for personal communications, and the provision of legal services related to the requirements and compliance with US law (among others). It is important to analyse carefully the general licence specific to each country programme as the requirements and restrictions may vary from programme to programme. For example, the general licence for the export of agricultural commodities, medicine and medical devices to Iran, set forth in the ITSR, includes authorisations only for certain 'covered persons' and excludes the export of some specified goods.[7] Furthermore, some sanctions programmes contain general licences authorising the export of certain goods or services that are highly tailored to a specific country and its respective sanctions programme and that do not appear in any form in other country sanctions programmes. For example, Cuba and Venezuela have highly individualised sets of general licences that change frequently and are specific to the unique sanctions programme for each country.

Specific licences are granted case by case under certain limited situations and conditions. Requests for specific licences may be submitted directly to OFAC. These licences will typically be granted only if the activity is in the interest of US foreign policy.

45.1.4 Key jurisdictions

As noted above, the United States maintains comprehensive sanctions on Cuba, Iran, North Korea, Syria and the Crimea Region of Ukraine. Additionally, OFAC imposes significant sanctions on state-owned entities in Russia and the government of Venezuela.

45.1.4.1 Cuba

The comprehensive sanctions on Cuba, governed by the Cuban Assets Control Regulations (CACR),[8] generally prohibit any transaction by a person subject to US jurisdiction, including foreign entities owned or controlled by a US person, in which Cuba or a Cuban national has an interest. This includes the export of goods and services, including financial services, to Cuba and the import of Cuban goods into the United States. US persons are also prohibited from approving, financing, facilitating or guaranteeing any transaction by a foreign person in which they would be prohibited from engaging themselves.

The CACR contains several general licences authorising activities supporting the Cuban people and private enterprise in Cuba.[9] Additionally, the

7 31 CFR §§ 560.530 (3)(ii), 560.530 (4).

8 31 CFR Part 515.

9 31 CFR §§ 515.502 to 515.591.

© Law Business Research 2021

CACR currently contains general licences regarding travel-related transactions for a variety of specified activities. All general licences should be checked frequently to confirm that relevant authorisations are still in effect and that additional restrictions or requirements have not been placed, limiting the scope of the general licences.

Iran 45.1.4.2

OFAC's sanctions programme on Iran is primarily governed by the ITSR.[10] The Regulations generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to Iran and US person facilitation of those prohibited transactions. The prohibitions in the ITSR also apply to foreign entities owned or controlled by a US person.

OFAC reimposed significant secondary sanctions that threaten sanctions on non-US persons for certain transactions involving Iranian SDNs and for specified activities in key sectors of the Iranian economy following the United States' withdrawal from the JCPOA on 8 May 2018.[11] With the issuance of Executive Order 13902 in January 2020, even more sectors of the Iranian economy became the subject of secondary sanctions, meaning that most trade with Iran now potentially carries secondary sanctions exposure.[12]

North Korea 45.1.4.3

The North Korean Sanctions Regulations[13] generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to North Korea and facilitation of those prohibited transactions by US persons.

In addition to the primary sanctions detailed above, a number of North Korea-related executive orders authorise the imposition of secondary sanctions on persons determined to be engaging in certain specified commercial activities involving North Korea.[14]

Syria 45.1.4.4

The Syrian Sanctions Regulations[15] generally prohibit the export, re-export, sale or supply, directly or indirectly, from the United States or by a US person,

10 31 CFR Part 560.

11 Exec. Orders 13902 and 13871 authorise the imposition of secondary sanctions on specified transactions involving Iran's iron, steel, aluminium copper, construction, mining, manufacturing and textile sectors. See Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 Jan. 2020); Exec. Order No. 13871, 84 Fed. Reg. 20761 (10 May 2019).

12 See Exec. Order No. 13902, 85 Fed. Reg. 2003 (10 Jan. 2020).

13 31 CFR Part 510.

14 Exec. Order No. 13810, 82 Fed. Reg. 44705 (20 Sep. 2017).

15 31 CFR Part 542.

© Law Business Research 2021

wherever located, of any services to Syria and US person facilitation of those prohibited transactions.

Additionally, Section 7412 of the National Defense Authorization Act for Fiscal Year 2020 (also titled the Caesar Syria Civilian Protection Act of 2019) authorised sanctions against any foreign person determined to knowingly provide significant financial, material or technological support to, or knowingly engage in a significant transaction with, certain persons in Syria, primarily relating to the government of Syria and its military or any foreign person subject to sanctions with respect to Syria.[16]

45.1.4.5 Crimea region of Ukraine

The Ukraine-Related Sanctions Regulations generally prohibit the export re-export, sale or supply, directly or indirectly, from the United States or by a US person, wherever located, of any goods, technology or services to Crimea and facilitation of those prohibited transactions by US persons.[17]

45.1.4.6 Russia

Russia is not subject to a comprehensive embargo but to significant targeted sectoral sanctions on persons in identified sectors of Russia's economy, although a number of Russian persons also appear on OFAC's SDN List. In addition, pursuant to Executive Order 13662,[18] OFAC issued Directives 1 to 4 imposing sectoral sanctions against entities identified on OFAC's SSI List[19] operating in certain sectors of the Russian economy, such as financial services, energy and defence.[20]

Directives 1 to 3 contain prohibitions on dealing in new debt with a maturity longer than that defined in the Directive or, for Directive 1, new equity on behalf of designated Russian entities operating in Russia's financial, energy and defence sectors. Directive 1 was expanded by Executive Order 14024, published on 15 April 2021, to prohibit US financial institutions from participating in the primary market for rouble or non-rouble denominated funds by, or the lending of rouble or non-rouble denominated funds to Russia's Central Bank, National Wealth Fund or Ministry of Finance.[21]

Directive 4 prohibits the export or re-export by a US person, directly or indirectly, of goods, services or technology in support of deep-water, Arctic offshore or shale projects, including new projects outside Russia in which an entity subject to Directive 4 has an ownership interest of 33 per cent or more.

---

16 Caesar Civilian Protection Act, Section 7412(2) of the National Defense Authorization Act for Fiscal Year 2020.

17 31 CFR Part 589.

18 Exec. Order No. 13662, 79 Fed. Reg. 16169-71 (24 Mar. 2014).

19 The SSI List is available at https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/sectoral-sanctions-identifications-ssi-list.

20 Exec. Order No. 13662, 79 Fed. Reg. 16167 (20 Mar. 2014).

21 OFAC FAQ #890; See also, Exec. Order No. 14024, 86 Fed. Reg. 20249 (15 Apr. 2021).

© Law Business Research 2021

Companies engaging in transactions with SSI entities should scrutinise payment terms to ensure that they do not violate the requirements of the applicable Directive.

The United States also maintains secondary sanctions on Russia. The Countering America's Adversaries Through Sanctions Act (CAATSA) mandates the imposition of sanctions against persons that the President determines have knowingly facilitated a 'significant transaction'[22] for or on behalf of any person subject to sanctions imposed by the United States with respect to the Russian Federation, including for or on behalf of a Russian person or entity on OFAC's SDN List.[23] OFAC has effectively limited this threat of sanctions to transactions with any Russian person on its SDN list.[24]

CAATSA also mandates that the President impose sanctions on persons determined to have knowingly engaged in a significant transaction with a person involved in the intelligence or defence sectors of the Russian government. The Department of State published the List Regarding the Defense Sector of the Government of the Russian Federation[25] of persons determined to be part of, or operating for or on behalf of, Russian defence or intelligence sectors.[26]

Finally, CAATSA also mandates that the President impose sanctions on persons determined to have made significant investments above a specified threshold that directly and significantly contribute to Russia's ability to construct energy export pipeline projects initiated on or before 2 August 2017, or that provide significant goods, services, technology, information or support to directly and significantly facilitate the maintenance or expansion of the construction, modernisation or repair of energy export pipelines.[27]

Venezuela 45.1.4.7

Executive Order 13884 blocks all property and interests in property of the government of Venezuela.[28] This means that US persons are generally prohibited from engaging in any transaction in which the government of Venezuela has an interest, including with entities of which 50 per cent or more is owned by the government of Venezuela.

Additionally, Executive Order 13850 blocks the property of additional persons who may be contributing to the situation in Venezuela, including those operating in specified sectors of the Venezuelan economy as determined

22 See discussion on 'significant transactions', supra note 6.

23 See Countering America's Adversaries Through Sanctions Act [CAATSA] § 228.

24 OFAC FAQ #541.

25 The US Department of State's List Regarding the Defense Sector of the Government of the Russian Federation can be found at https://www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation/.

26 See CAATSA § 231.

27 CAATSA § 232.

28 Exec. Order No. 13884, 84 Fed. Reg. 38843 (6 Aug. 2019).

© Law Business Research 2021

by the Secretary of the Treasury.[29] Notably, OFAC designated the Venezuelan state oil company, Petróleos de Venezuela SA, pursuant to this authority on 28 January 2019.

OFAC has published several general licences authorising certain activities by US persons that would otherwise be prohibited by the Venezuela-related sanctions programme. A majority of these general licences change frequently and are very specific as to what actions they authorise and to whom they apply. As such, companies should ensure they scrutinise and carefully monitor any general licence relied on to conduct business otherwise prohibited by the Venezuela-related Executive Orders.

45.2 Offences and penalties

See Chapter 26 on fines, disgorgement, etc.

Generally, US primary sanctions prohibit transactions only by US persons or transactions subject to US jurisdiction. For Cuba and Iran, the restrictions also apply to foreign entities that are owned or controlled by a US person. 'Owned or controlled' is understood to encompass holding at least 50 per cent of the equity interest by vote or value, a majority of seats on the board of directors, or otherwise controlling actions, policies and personnel decisions of the foreign entity.[30]

Although non-US companies are generally not themselves required to comply with OFAC regulations, they can still face potential liability for exporting goods or services from the United States to a target of US sanctions or for 'causing a violation' by involving a US person in a transaction that would be prohibited for that US person.[31] The most typical way that such a violation by a non-US person might occur is if a transaction involving a target of US sanctions is denominated in US dollars because most US dollar transactions clear through US banks and therefore involve the services of a US financial institution.[32]

29 Exec. Order No. 13850, 83 Fed. Reg. 55243 (2 Nov. 2018).

30 31 CFR §§ 515.329, 560.215. For example, in 2019, OFAC entered enforcement proceedings against General Electric regarding apparent violations by three of its non-US subsidiaries for accepting payments from a party owned by the Cuban government and on OFAC's SDN List. See 'OFAC Enforcement Information for October 1, 2019', The General Electric Company, available at https://home.treasury.gov/system/files/126/20191001_ge.pdf.

31 50 USC § 1705.

32 One example can be found in OFAC's enforcement action against Standard Chartered Bank (SCB), a financial institution headquartered in the United Kingdom. In 2019, SCB entered into a global settlement with OFAC and other US federal agencies for processing transactions involving persons or countries subject to comprehensive sanctions. The majority of the transactions concerned Iran-related accounts maintained by SCB's Dubai branches that processed US dollar transactions through SCB's branch office in New York or other US financial institutions. See 'OFAC Enforcement Information for April 9, 2019', Standard Chartered Bank, available at https://home.treasury.gov/system/files/126/20190408_scb_webpost.pdf.

© Law Business Research 2021

Under secondary sanctions, access by a non-US company to US markets or the US financial system may be restricted, including by being added to the SDN List, if it engages in certain conduct relating to Iran, Russia or North Korea.

Commencement of sanctions investigations 45.3

The US government can learn of a potential sanctions violation in a number of ways, including through voluntary self-disclosure (VSD), a report of a blocked or rejected transaction, referral from another government agency and even publicly available information, such as a media report.

If a company learns of a potential violation, it may submit a VSD to OFAC. This has many benefits, including a significant reduction in the base penalty for a potential enforcement action. However, parties should carefully consider whether to file based on the circumstances of and facts surrounding the potential violation and their history of engagement with OFAC.

In addition to VSDs, the US government often learns of potential violations through blocked or rejected transaction reports filed by US persons, typically financial institutions, based on suspected sanctions violations. Since June 2019, all US persons must submit reports to OFAC within 10 business days of blocking or rejecting a transaction.[33] Previously, all parties had to report transactions involving blocked property to OFAC, but only US financial institutions were obliged to report rejected transactions.[34]

OFAC may also learn of sanctions violations through anti-money laundering reports, primarily suspicious activity reports, or through criminal investigations conducted by the DOJ or other federal and state law enforcement agencies.

On learning of a potential violation, OFAC may send an initial request for information to the parties with an administrative subpoena or, depending on the nature of the violation, send an informal set of questions to the involved parties, including non-US persons.

Enforcement 45.4

Factors to consider 45.4.1

The test in the United States for civil enforcement of sanctions is one of strict liability. This means that companies can be liable for sanctions violations without proof of knowledge, fault or intent, highlighting the importance of sanctions compliance programmes. Parties should also determine whether there was a wilful violation of US sanctions laws that could lead to a criminal investigation or enforcement action. Parties should balance the need to move

33 See 31 CFR § 501.603.

34 An example of OFAC learning of a potential violation through a blocked transaction report can be found in the enforcement action against Hotelbeds USA. OFAC was notified of the apparent violations through a blocked payment report filed by a US financial institution related to a Cuba-travel related transaction. See OFAC 'Enforcement Information for June 13, 2019', at https://home.treasury.gov/system/files/126/20190612_hotelbeds_0_1.pdf.

© Law Business Research 2021

quickly after identifying a potential violation with taking the time to understand the nature of the violation to determine whether a VSD is appropriate and to whom the parties should report.

45.4.2 Compliance framework

In May 2019, OFAC issued its Framework for Compliance Commitments.[35] This guidance document encourages a risk-based approach, noting that no single compliance programme is suitable for every institution. However, the document provides five components that OFAC highlights as essential to any effective compliance programme:

- management commitment;
- risk assessment;
- internal controls;
- testing and auditing; and
- training.

Since publishing the Framework, OFAC has highlighted the importance of an effective risk-based compliance programme and reserved the final paragraph of published enforcement actions to discuss how the facts relate to the Framework and how both the party subject to the enforcement actions and other businesses in its industry can mitigate risks by implementing compliance policies and procedures proportional to the risks faced by the party and industry as a whole.[36] OFAC has indicated that the strength of a party's compliance programme can also be a significant mitigating or aggravating factor that it will consider when calculating a penalty amount.[37]

To further mitigate sanctions risks, parties should also ensure that their compliance programme meets the criteria presented in the DOJ's 'Evaluation

35 'A Framework for OFAC Compliance Commitments' is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

36 See 'OFAC Enforcement Information for February 26, 2020', Société International de Télécommunications Aéronautiques SCRL, available at https://home.treasury.gov/system/files/126/20200226_sita.pdf ('As noted in OFAC's Framework for Compliance Commitments issued in May 2019, companies can mitigate sanctions risks by conducting risk assessments and exercising caution when engaging in business transactions with entities that are affiliated with, or known to transact with, OFAC-sanctioned persons or jurisdictions, or otherwise pose high risks due to their joint ventures, affiliates, subsidiaries, customers, suppliers, geographic location, or the products and services they offer').

37 In OFAC's enforcement action against Haverly Systems for violations of the Ukraine Related Sanctions Regulations, OFAC considered the fact that Haverly did not have a formal OFAC sanctions compliance programme at the time the apparent violations occurred was an aggravating factor. See 'OFAC Enforcement Information for April 25, 2019', available at https://home.treasury.gov/system/files/126/20190425_haverly.pdf.

© Law Business Research 2021

of Corporate Compliance Programs'.[38] The DOJ will evaluate a party's compliance programme when determining whether to impose a monitor on the party once an enforcement action relating to an apparent violation of US sanctions laws is concluded.

Best practices 45.4.3

Once an investigation has commenced, parties should proactively collaborate and co-operate with the agency conducting the investigation. OFAC enforcement actions and enforcement guidelines highlight co-operation as a mitigating factor to be taken into account in an enforcement action.[39] Furthermore, if the DOJ is conducting an investigation relating to a wilful violation of US sanctions, the party must fully co-operate with the DOJ to receive the benefits associated with submitting a VSD. Generally, full co-operation includes internal investigations to discover the root cause of an apparent violation, responding to regulators' requests for additional information in a timely and complete manner, preserving all sensitive or relevant documents, and collaborating with regulators to develop and implement effective remedial measures.[40]

Once an investigation has commenced, under no circumstances should parties attempt to hide or destroy material information or evidence. Any indication that the parties have attempted to oppose an investigation is likely to lead federal and state investigators into taking a more hostile approach.

Self-reporting to OFAC 45.4.3.1

OFAC generally views VSDs favourably and a VSD will reduce the base penalty of an apparent violation by up to 50 per cent. To be considered voluntary, a disclosure must be self-initiated and submitted to OFAC before it or any other government agency or official discovers the apparent violation. One exception is that a VSD to another government agency may be considered a VSD to OFAC, case by case. A VSD to OFAC must include, or be followed by, a report containing sufficient details to provide a complete understanding of the circumstances of the apparent violation. In some instances, it may be beneficial to the party to make a preliminary disclosure to OFAC before knowing all the

38 The DOJ's 'Evaluation of Corporate Compliance Programs' is available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

39 For example, in OFAC's enforcement action against Stanley Black & Decker, Inc and its subsidiary, OFAC found that Stanley Black & Decker's co-operation with OFAC, including an extensive internal investigation and meaningful responses to OFAC's requests for additional information, was a mitigating factor when determining the penalty amount. See OFAC 'Enforcement Information for March 27, 2019', available at https://home.treasury.gov/system/files/126/20190327_decker.pdf.

40 For guidance on co-operating with OFAC, see 31 CFR 501 Appendix A(III)(G). For guidance on the requirements necessary for credit for full co-operation with a DOJ sanctions-related investigation, see DOJ Export Control and Sanctions Enforcement Policy for Business Organizations, pp. 3 to 5.

© Law Business Research 2021

facts to be timely and ensure disclosure is considered voluntary. Parties should ensure that their VSD and follow-up report contain all the details known at the time they are made and be prepared to respond to any follow-up enquiries.[41]

OFAC's enforcement guidelines list several instances where notices will not be considered a VSD, including licence applications, notifications from a third party of an apparent violation or substantially similar apparent violation because it blocked or rejected a transaction, or if the disclosure:

- includes false or misleading information or is materially incomplete;
- is not self-initiated;
- is made without the authorisation of senior management; or
- is in response to an administrative subpoena or other enquiry form.[42]

45.4.3.2 Self-reporting to the DOJ

The DOJ's VSD policy, published on 13 December 2019, states that all business organisations, including financial institutions, are eligible for all the benefits detailed by the policy.[43] Similar to other DOJ self-disclosure policies, companies are eligible for the benefits of the updated VSD policy when they (1) voluntarily self-disclose export control or sanctions violations to the National Security Division's Counterintelligence and Export Control Section (CES), (2) fully co-operate with the investigation and (3) remediate any violations appropriately and in a timely manner. The threshold for eligibility is self-disclosure of potential violations to CES. Unlike with OFAC, self-disclosing to any other regulatory agency is not considered an eligible VSD to the DOJ under its new policy.[44] Accordingly, to obtain the benefit of self-disclosure in a criminal investigation, parties must disclose to DOJ before OFAC.

For a party's disclosure to be considered voluntary, it must be made before there is an imminent threat of disclosure or government investigation, and reasonably promptly after discovery of the offence. Further, the party must disclose all relevant facts known to it at the time of the disclosure.[45] To receive credit for full co-operation, parties are required to:

- disclose all relevant facts in a timely manner;
- co-operate proactively with the DOJ;
- preserve, collect and disclose all relevant documents and information;
- deconflict witness interviews when required; and
- make officers and employees of the party available for interviews by the DOJ when so requested.[46]

---

41 31 CFR 501 Appendix A(I)(I).

42 Id.

43 The DOJ's 'Export Control and Sanctions Enforcement Policy for Business Organizations' is available at https://www.justice.gov/nsd/ces_vsd_policy_2019/download.

44 Id. at p. 3.

45 Id.

46 Id. at pp. 3 to 5.

© Law Business Research 2021

Finally, parties are required to demonstrate a thorough analysis of the causes of underlying conduct and, where appropriate, engage in remediation; implement an effective compliance programme; discipline employees identified by the party as responsible for the oversight; retain business records and prohibit the improper destruction of those records; and take any additional steps that demonstrate recognition of the seriousness of a party's misconduct.[47]

Considerations

Submitting a VSD to OFAC can have several benefits, the most significant of which is that it is considered a mitigating factor in the calculation of a potential penalty amount. In some cases, a VSD can allow a party to avoid an enforcement action altogether if OFAC determines the conduct does not constitute a violation or that it does not warrant a civil monetary penalty. However, there are general costs associated with making a VSD to either OFAC or the DOJ, including legal expenses, government investigation, additional scrutiny, reputational harm and, in some cases, large monetary penalties. There is also the potential for a government investigation to reveal unknown or undisclosed violations.

When submitting a VSD to OFAC, in particular, parties should carefully consider the possibility that the conduct was wilful and that, as a result, OFAC may refer the case to the DOJ for criminal enforcement, removing the option to have a VSD accepted by the DOJ.

If a party submits a VSD to the DOJ that satisfies the requirements of its updated VSD policy, there is a presumption that the party will receive a non-prosecution agreement and pay no fine, in the absence of aggravating factors.[48] However, even if a party receives a non-prosecution agreement, at a minimum it will not be permitted to retain any of the unlawfully obtained gain and will be required to pay all disgorgement, forfeiture or restitution resulting from the misconduct.[49] Even if there are aggravating circumstances, the DOJ will still recommend a fine of at least 50 per cent less for a qualifying party than would have been levied in the absence of a VSD and will not require the imposition of a monitor if the party has implemented an effective compliance programme at the time of resolution.[50] By filing with the DOJ, a party may invite a criminal investigation in addition to heavy, continuing disclosure obligations.

See Chapter 4 on self-reporting to authorities

Overall, effective use of OFAC and the DOJ's VSD programmes rests in the strength of a party's compliance programme, policy and procedures. Even if the policy and procedures fail to prevent an apparent violation, they can help parties quickly and more accurately determine the nature of the violation and whether a VSD to OFAC or the DOJ is necessary and beneficial.

47 Id. at pp. 5 to 6.

48 Id. at pp. 2 to 3.

49 Id.

50 Id.

© Law Business Research 2021

Other government authorities

In addition to OFAC and the DOJ, parties should also consider notifying potential violations to relevant US and non-US regulators, shareholders, counterparties, insurers and other interested parties. Parties should also be aware that OFAC maintains memoranda of understanding with several state and federal banking regulatory agencies, which may impose penalties on financial institutions in connection with apparent violations of US sanctions laws.[51] As such, financial institutions should consider notifying their regulators of potential violations. Parties should also determine whether the potential violation of US sanctions laws also violates sanctions laws in foreign jurisdictions and whether it would be appropriate to make disclosures to the relevant regulatory bodies. All these considerations should be made while conscious of the requirements for VSD submissions to OFAC and the DOJ, namely, when a VSD is no longer considered eligible for the benefits.

45.4.3.3 Settlement

OFAC enforcement actions often end in settlement. Settlement discussions may be initiated by either OFAC or the party committing the apparent violation at several points during the enforcement process. These settlements can also include multiple violations or be a part of a comprehensive settlement with other federal, state or local agencies that are also pursuing investigations or enforcement actions relating to the apparent violation.[52]

45.5 Trends and key issues

45.5.1 Recent enforcement activity

Since the release of its Framework for Compliance Commitments in May 2019, OFAC has been able to map compliance programmes against the Framework to determine whether a party's compliance programme should be considered an aggravating or mitigating factor. For example, in an enforcement action against Eagle Shipping International, OFAC stated that:

> *[a]s noted in OFAC's Framework for Compliance Commitments, this case demonstrates the importance for companies operating in high-risk industries (e.g., international shipping and trading) to implement risk-based*

51 The Department of the Treasury maintains a list of memoranda of understanding between OFAC and state and federal banking regulators at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information/memoranda-of-understanding-between-ofac-and-bank-regulators.

52 One example of this is UniCredit Bank AG agreeing to pay approximately US$611 million to OFAC as part of a US$1.3 billion settlement with federal and state government partners. See, e.g., US Department of the Treasury press release, 'US Treasury Department Announces Settlement with UniCredit Group Banks' (15 April 2019), available at https://home.treasury.gov/news/press-releases/sm658.

© Law Business Research 2021

compliance measures, especially when engaging in transactions involving exposure to jurisdictions or persons implicated by US sanctions.[53]

Recent enforcement activity has also shown that OFAC is willing to use a minimal or indirect nexus to the United States to proceed with an enforcement action against a non-US party.[54] OFAC has also showed its willingness to expand its extraterritorial jurisdiction to penalise non-US companies for transactions that would not have been covered by OFAC's jurisdiction if not for the use of servers located in the United States.[55] Late 2020 also saw OFAC publish its first enforcement actions targeting apparent violations of US sanctions laws in the cryptocurrency industry.[56]

See Chapter 28 on extraterritoriality

53 See OFAC 'Enforcement Information for January 27, 2020', Eagle Shipping International, available at https://home.treasury.gov/system/files/126/20200127_eagle.pdf.

54 For example, the enforcement action against British Arab Commercial Bank (BACB), OFAC considered even tenuous and indirect contact with US financial institutions as grounds for an enforcement action. OFAC found that BACB had violated Sudanese sanctions despite the fact that the transactions at issue were not processed to or through the US financial system. BACB operated a nostro account in a country that imports Sudanese-origin oil for the stated purpose of facilitating payments involving Sudan. The bank funded the nostro account with large, periodic US dollar wire transfers from banks in Europe, which in turn transacted with US financial institutions in a manner that violated OFAC sanctions. See OFAC 'Enforcement Information for September 17, 2019', British Arab Commercial Bank, available at https://home.treasury.gov/system/files/126/20190917_bacb.pdf.

55 For example, the enforcement action against Société Internationale de Télécommunications Aéronautiques SCRL (SITA), OFAC's basis for jurisdiction over SITA, a global information technology services provider headquartered in Switzerland and serving commercial air transportation, was that the technology provided to sanctioned parties was hosted on, and incorporated functions that routed messages through, US servers and contained US-origin software. See OFAC 'Enforcement Information for February 26, 2020', Société Internationale de Télécommunications Aéronautiques SCRL, available at https://home.treasury.gov/system/files/126/20200226_sita.pdf.

56 For example, enforcement action against BitGo, Inc., OFAC signalled its intent to enforce sanctions compliance in the cryptocurrency industry. The apparent violations involved users located in sanctioned jurisdictions signing up for and accessing BitGo's secure digital wallet management services to engage in digital currency transactions. Despite having access to the IP addresses of its customers, tracked at the time for security purposes related to logins, BitGo did not use that information for sanctions compliance purposes. OFAC highlighted the importance of entities involved in providing digital currency services to implement sanctions compliance controls commensurate with their risk profile. The fact that BitGo did not implement appropriate, risk-based sanctions compliance controls and had reason to know the users were located in sanctioned jurisdictions based on their IP addresses were seen as aggravating factors. See OFAC 'Enforcement Information for December 30, 2020', at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

© Law Business Research 2021

45.5.2 Potential pitfalls

Companies should be wary of OFAC's continued use of increasingly indirect and tenuous links to the US financial system to bring enforcement actions against foreign parties for 'causing a violation' by US banks. As such, non-US companies should scrutinise the structure of transactions to or with persons or countries subject to US sanctions to ensure that there are no potential direct or indirect links to the US financial system, including transactions that use US dollars. Additionally, given the emphasis OFAC places on its Framework for Compliance Commitments, companies should ensure that their compliance programmes are in line with the Framework.

© Law Business Research 2021

46

Compliance

Alison Pople QC, Johanna Walsh and Mellissa Curzon-Berners[1]

Introduction 46.1

Compliance issues are at the heart of the vast majority of financial crime and misconduct investigations, and subsequent criminal and regulatory enforcement action. Accordingly, many international government enforcement bodies have sought to articulate formally what is required for effective compliance. In the United Kingdom, corruption, facilitation of tax evasion and money laundering are among the more evolved areas, with the relevant guidance also offering assistance on other specific areas of legal risk. In the United States, corruption and antitrust are two areas where detailed and extensive guidance is available.

Alongside the available guidance offered by international government enforcement bodies, there is an evolving body of criminal and regulatory enforcement outcomes in the United Kingdom, United States and other jurisdictions that address compliance issues. Investigations practitioners can draw on this material to prepare and promote new policies for a corporate, analyse potential compliance issues within an investigation, prepare for potential future criminal or regulatory proceedings where compliance is a central issue and make timely remediation where compliance failures have occurred.

The international corporate compliance landscape is vast, and it is beyond the scope of this chapter to examine in detail the legal and regulatory requirements across all sectors and jurisdictions. This chapter focuses principally on the UK position concerning offences and defences, and reviews the key areas of risk arising from compliance failures and available corporate defences. It draws

1 Alison Pople QC is a barrister at Cloth Fair Chambers. Johanna Walsh is a partner, and Mellissa Curzon-Berners is an associate, at Mishcon de Reya LLP.

© Law Business Research 2021

on the compliance guidance in the United Kingdom and the United States and analyses the impact of compliance on investigatory outcomes. It explores the interplay between culture and compliance, the merits of the US Foreign Corrupt Practices Act (FCPA) Opinion Procedure and, finally, draws on the compliance lessons arising from a variety of UK and US cases.

Practitioners should be mindful of the breadth of compliance issues that may be engaged in a number of jurisdictions in any single investigation, particularly when dealing with multinational corporates operating in high-risk sectors. The insight provided by the UK and US guidance and the lessons learned from the outcomes to date, may also resonate in other jurisdictions, particularly in cross-border investigations.

46.2 UK criminal liability for corporate compliance failures

46.2.1 Section 7 Bribery Act 2010

The implementation of the section 7 offence in July 2011 represented a move away from corporate criminal liability via 'the identification principle' towards liability through 'failure to prevent' offences.[2] By section 7(1) Bribery Act 2010, a 'relevant commercial organisation'[3] commits an offence if a person associated with it bribes another person intending to get or keep business, or an advantage in the conduct of business, for the organisation. However, by section 7(2), a company can rely on compliance as a defence to a criminal offence. An organisation that had 'adequate procedures designed to prevent persons associated with [the organisation] from undertaking such conduct' will have a defence to the section 7 offence.

See Chapter 1

The majority of section 7 cases in England have been resolved through deferred prosecution agreement (DPA). The Crown Court has approved DPAs for section 7 offences between the Serious Fraud Office (SFO) and Standard

See Chapter 23 on negotiating global settlements

2 On 3 November 2020, the UK Ministry of Justice published the government's response to its 'Corporate liability for economic crime: call for evidence', which ran between January 2017 and March 2017. It reported that the evidence received was inconclusive and that the government was not persuaded there was a sufficient evidence base on which to make immediate legislative change. Instead, in November 2020, the government asked the Law Commission to examine the issue of corporate criminal liability and provide an assessment of the different options for reform. On 9 June 2021, the Law Commission published 'Corporate Criminal Liability: A discussion paper', which invites responses to 13 questions for discussion. Following the consultation, the Law Commission will proceed to policy development and advice to government, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/06/Corporate-Criminal-Liability-Discussion-Paper.pdf.

3 A 'relevant commercial organisation' is defined at s.7(5) Bribery Act as a body or partnership that is incorporated or formed in any part of the United Kingdom irrespective of where it carries on a business, or any other incorporated body or partnership which carries on a business or part of a business in the United Kingdom irrespective of the place of incorporation or formation.

© Law Business Research 2021

Bank plc,[4] Sarclad Ltd,[5] Rolls-Royce plc and Rolls-Royce Energy Systems Inc,[6] Güralp Systems Ltd,[7] Airbus SE,[8] Airline Services Ltd,[9] Amec Foster Wheeler Energy Ltd[10] and two other companies (AB Ltd and CD Ltd[11]). One company, Sweett Group plc,[12] has pleaded guilty to a section 7 offence. There has been just one contested section 7 prosecution in a Crown Prosecution Service (CPS) case against Skansen Interiors Ltd,[13] where Skansen pursued an adequate procedures defence but was subsequently convicted.

Sections 45 and 46 Criminal Finances Act 2017 46.2.2

The Criminal Finances Act 2017 introduced the offences of failure to prevent the facilitation of UK tax evasion and failure to prevent the facilitation of foreign tax evasion. These offences hold a 'relevant body'[14] criminally liable when a person associated with it commits either a UK tax evasion facilitation offence (pursuant to section 45) or a foreign tax evasion facilitation offence (pursuant to section 46). In respect of the section 46 offence, one of three alternative jurisdiction conditions[15] must also be satisfied.

Compliance-based defences are available for both offences[16] if the corporate defendant can prove that 'it had in place such reasonable prevention procedures it was reasonable in all the circumstances to have in place' or 'that it was not reasonable in all the circumstances to expect [the relevant body] to have any prevention procedures'.

To date there have been no prosecutions for either of these offences. As at 27 May 2021, there were 14 live investigations with a further 14 'opportunities' under review across 10 business sectors, including financial services,

4 *SFO v. Standard Bank plc (now ICBC Standard Bank plc)*, Crown Court (Southwark), 30 November 2015 [2016] Lloyd's Rep FC 102 (*Standard Bank*).

5 *SFO v. Sarclad Ltd*, Crown Court (Southwark), 8 July 2016, Case No. U20150856 (*Sarclad*).

6 *SFO v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc*, Crown Court (Southwark), 17 January 2017 [2017] Lloyd's Rep FC 249 (*Rolls-Royce*).

7 *SFO v. Güralp Systems Ltd*, Crown Court (Southwark), 22 October 2019 [2020] Lloyd's Rep FC 90 (*Güralp*).

8 *SFO v. Airbus SE*, Crown Court (Southwark), 31 January 2020, Case No. U20200108 (*Airbus*).

9 *SFO v. Airline Services Limited*, 30 October 2020, Case No. U20201913 (*Airline Services Ltd*).

10 *SFO v. Amec Foster Wheeler Energy Limited*, 1 July 2021 (*Amec Foster Wheeler*).

11 The final hearing was concluded on 19 July 2021 at the Royal Courts of Justice (listed as *SFO v .AB Ltd and CD Ltd*). Reporting restrictions apply under the Contempt of Court Act 1981 in respect of aspects of these proceedings. The full documentation (deferred prosecution agreements, statements of facts and judgment) will only be published once those restrictions have been lifted.

12 *R. v. Sweett Group plc* (unreported).

13 *R. v. Skansen Interiors Ltd* (unreported) (*Skansen*).

14 A 'relevant body' is defined at s.44(2) as a body corporate or partnership (wherever incorporated or formed). Partnership is separately defined at s.44(3).

15 As set out in Criminal Finances Act 2017, s.46(2).

16 See ibid., ss.45(2) and 46(3).

© Law Business Research 2021

oils, construction, labour provision and software development embracing a full range of corporate entities from small businesses through to some of the United Kingdom's largest organisations.[17]

46.2.3 Compliance-based distinctions between failure-to-prevent offences

A distinction between the failure-to-prevent offences in the Bribery Act and Criminal Finance Act, which otherwise follow a similar concept of corporate criminal liability, is found in the description of the standard of prevention procedures governing the availability of the statutory defences, namely 'adequate procedures' compared to prevention procedures that are 'reasonable in all the circumstances'. It has been argued that the 'adequate procedures' standard might be considered a stricter standard, with the effect that where an underlying bribery offence is proved, the prevention procedures must of necessity not have been 'adequate'. This might be the case notwithstanding the presence of procedures that were 'reasonable in all the circumstances' but were circumvented on a particular occasion. Given this potential unintended consequence, attempts were made to replace 'adequate procedures' with 'reasonable procedures in all the circumstances' during the passage of the Bribery Bill through Parliament, but these were unsuccessful. The argument was revisited in post-legislative scrutiny by a House of Lords select committee.[18] The committee decided that the danger of an overly strict interpretation of 'adequate procedures' was unlikely, and statutory amendment of section 7(2) was unnecessary. However, it did recommend changes to the Bribery Act Guidance[19] 'to draw attention to the different wording in the Criminal Finances Act 2017 and in the HMRC Guidance to that Act, and to make clear that 'adequate' does not mean, and is not intended to mean, anything more stringent than 'reasonable in all the circumstances'.

There has been no change to the Bribery Act Guidance in this, or any other respect. Another relevant distinction is that the Criminal Finances Act offences specifically contemplate and provide for a defence in circumstances in which it is reasonable for a corporate to have no prevention procedures in place.

46.2.4 Regulation 86 Money Laundering Regulations 2017

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLTF Regulations) target the

17 See HMRC Freedom of Information Act release dated 26 May 2021 on the number of live corporate criminal offences investigations.

18 House of Lords Select Committee on the Bribery Act 2010, report of Session 2017-19 'The Bribery Act 2010: post-legislative scrutiny'.

19 Ministry of Justice guidance on the Bribery Act 2010 issued pursuant to s.9 of that Act.

© Law Business Research 2021

'gatekeepers' of the UK financial system. These 'relevant persons'[20] must have policies, controls and procedures to mitigate the risks of money laundering and terrorist financing.

See Chapter 3 on self-reporting to the authorities

The MLTF Regulations are deliberately non-prescriptive. They require corporates to tailor their compliance policies according to their individual risk-profile. The requirements extend to ensuring that employees and agents (at group and subsidiary level) are aware of the law relating to money laundering and terrorist financing, are trained appropriately and take proportionate steps to reduce the risks within the ordinary course of their relevant business activities.

Failure to comply with the requirements of the MLTF Regulations is a criminal offence.[21] In deciding whether a corporate has committed an offence, the court will consider whether it followed any relevant guidance, including from the Financial Conduct Authority (FCA) and other supervisory authorities. No offence is committed where a corporate can demonstrate that it took 'all reasonable steps' and 'exercised all due diligence' to avoid committing it.[22]

To date, there have been very few criminal convictions for a breach of the MLTF Regulations.[23]

UK regulatory liability for corporate compliance failures 46.3

The FCA 46.3.1

The FCA Principles[24] embody the fundamental precepts that regulated businesses are expected to uphold. Firms must conduct their business with integrity (Principle 1) and due skill, care and diligence (Principle 2), and take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems (Principle 3).

---

20 Regulations 3(1) and 8 – A firm will be a 'relevant person' if it falls within the MLTF Regulations' definitions of (1) credit institutions, (2) financial institutions, (3) auditors, insolvency practitioners, external accountants and tax advisers, (4) independent legal professionals, (5) trust or company service providers, (6) estate agents and lettings agents, (7) high value dealers, (8) casinos, (9) art market participants, (10) cryptoasset exchange providers, and (11) custodian wallet providers.

21 Regulation 86.

22 Regulation 86(3).

23 HM Treasury reported three convictions in cases brought by HMRC in its 'Anti-money laundering and counter-terrorist financing: supervision report 2018-2019', published August 2020. The limited number of prosecutions may be set to change. In its 2020/21 Business Plan, the FCA emphasises a shift in focus towards firms that fail to meet the required standards. Following this, on 16 March 2021, the FCA announced that it had launched criminal proceedings against National Westminster Bank plc in respect of offences under the Money Laundering Regulations 2007. This is the first prosecution brought by the FCA in respect of these regulations. Similarly, in its consultation on the 2020–2023 Business Plan, the Solicitors Regulation Authority notes that money laundering 'has increasingly become a priority area for us and one in which we robustly scrutinise those we regulate'.

24 FCA Handbook, PRIN 2.

© Law Business Research 2021

In addition to the Principles, the FCA Handbook contains a number of binding rules relevant to corporate compliance. Commentary on the relevant guidance provided by the FCA is set out below.

Under the Financial Services and Markets Act 2000 (FSMA), the FCA has an extensive range of disciplinary, criminal and civil powers to take action against businesses and individuals that fail to meet the required standards. These include withdrawing a firm's authorisation, suspending a firm from undertaking specified regulated activities, imposing a financial penalty and pursuing a criminal prosecution.

See Chapters 3 on self-reporting to the authorities and 25 on fines, disgorgement, etc.

The FCA is principally active in the civil enforcement regime. For example, in February 2019, the FCA fined Standard Chartered Bank (SCB) over £102 million for breaches of the Money Laundering Regulations 2007.[25] The FCA found that SCB had failed to establish and maintain adequate risk-sensitive policies and procedures and failed to apply UK-equivalent anti-money laundering (AML) standards to its branches and subsidiaries outside the European Economic Area, specifically within the United Arab Emirates. One of the key aggravating features in SCB's case was that its breaches occurred against a backdrop of 'heightened awareness' of deficiencies in its global financial controls. As early as 2013, group internal audit had identified that weaknesses in the escalation of AML risks from country to group level were impeding the board's ability to exercise adequate oversight of AML controls.[26]

46.3.2 Other professional regulators, specialist regulators

Practitioners should be aware that sector-specific and profession-specific regulators have also taken enforcement action against those they regulate for compliance breaches. These include the Financial Reporting Council, the Solicitors Regulation Authority, the Gambling Commission and the Groceries Code Adjudicator, to name but a few.

46.4 Compliance guidance

There is a wealth of compliance guidance available in the United Kingdom and the United States. The core guidance is summarised below and, as will be seen, there are a number of overlapping principles, with a particular focus on

25 Decision Notice, 5 February 2019.

26 The FCA also regularly takes civil enforcement action against regulated individuals for breaches of its Principles. For example, see the recent decision notice against Markos Theodosi Markou (Reference No. MXM01997), 29 January 2021, imposing a financial penalty of £25,000 and withdrawing approval to carry out senior management functions or any functions in relation to regulated activities, for reckless failure to, *inter alia*, establish, maintain and enforce effective crime systems and controls contrary to Principle 1. Similarly to SCB's case, an aggravating feature was that the FCA had 'repeatedly communicated serious concerns' in relation to the financial crime systems, controls and oversight, so that Mr Markou's conduct took place against a backdrop of 'obvious risk'. Mr Markou has referred the decision notice to the Upper Tribunal and it is therefore provisional.

© Law Business Research 2021

the importance of organisations having proportionate, risk-based procedures in place.

Examples of UK guidance 46.4.1

Bribery Act 46.4.1.1

The Ministry of Justice (MOJ) has published statutory guidance[27] addressing procedures that organisations can implement to prevent bribery.[28] The guidance aims to assist practitioners to assess or develop a compliance framework but is clear that whether any set of procedures is adequate for the purposes of the section 7 defence is a question of fact that can only be resolved by the courts.

The guidance is aimed at businesses of all sizes operating across all sectors and markets[29] and is founded on the following six principles, which are intended to be flexible and focused on outcomes.

- *Proportionate procedures*: Procedures should be proportionate to the level of bribery risk faced by each organisation, taking into account the nature, scale and complexity of that organisation's activities. They must be clear, practical, accessible, and effectively implemented and enforced.
- *Top-level commitment*: There must be a clear and demonstrable commitment to preventing bribery at the most senior levels. Top-level management must involve themselves in anti-bribery procedures, foster a culture of integrity and communicate, internally and externally, that bribery will never be accepted.
- *Risk assessment*: Organisations should regularly undertake an informed evaluation of the nature and extent of their bribery risk. These should address external risk (including country, sectoral, transaction, business opportunity and business partnership risk) and internal risk (including evaluating the sufficiency of employee training, skills and knowledge; bonus culture; gifts and hospitality policy; financial controls and the tone from the top).
- *Due diligence*: To mitigate bribery risk, due diligence must be applied (taking a proportionate and risk-based approach) to any persons who will or do perform services for or on behalf of the company. Due diligence should address the types of external and internal risk considered in regular

27 Bribery Act 2010, s.9(1):'The Secretary of State must publish guidance about procedures that relevant commercial organisations can put in place to prevent persons associated with them from bribing as mentioned in s7(1).'

28 https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

29 In post-legislative scrutiny of the Bribery Act, a House of Lords Select Committee concluded that the MOJ Guidance was less helpful in informing and advising small and medium-sized businesses on what would constitute an effective anti-bribery policy and stressed 'the importance for even the smallest companies of carrying out a properly documented risk assessment'. It recommended amending the Guidance to make this clear and to emphasise that all but the smallest businesses should have appropriately tailored procedures that staff have been trained to understand and follow.

© Law Business Research 2021

risk assessments. This is particularly important where the use of third-party intermediaries is contemplated.
- *Communication*: Policies and procedures must be well embedded through internal and external communication and regular training. The principle of proportionality applies.
- *Monitoring and review*: Organisations should keep under close review whether their procedures are still fit for purpose, having regard to any changes to the bribery risk faced or the nature and scale of their business.

Underpinning each principle is the need to document all steps taken to ensure that, in the event of an investigation, organisations can demonstrate that clear steps were taken to design and implement robust and appropriate procedures.

46.4.1.2 HMRC Facilitation of Tax Evasion Guidance

Guidance was published in September 2017 in respect of the Criminal Finances Act 2017 offences.[30] Critically it recognises that 'any regime that is risk-based and proportionate cannot also be a zero failure regime. If a relevant body can demonstrate that it has put in place a system of reasonable procedures that identifies and mitigates its tax evasion facilitation risks, then prosecution is unlikely as it will be able to raise a defence'. This offers reassurance that a corporate that produces reasonable procedures proportionate to its own risk will be protected from criminal prosecution and acts as a strong incentive to implement them. However, the emphasis is placed very specifically on accurate self-assessment and addressing of risk. It warns that it is not intended to provide 'safe-harbour' and makes clear 'even strict compliance with this guidance will not necessarily amount to having reasonable procedures, where the relevant body faces particular risks arising from the unique facts of its own business that remain unaddressed'.

The guidance is formulated around the same six guiding principles articulated in the Bribery Act Guidance. It puts considerable onus on a corporate to utilise the guidance and apply it meaningfully to its own circumstances, which will be affected by its size, nature and sector of business, and complexity and location of operations. It expressly does not provide a checklist and should 'be used to inform the creation of bespoke prevention procedures designed to address a relevant body's particular circumstances and the risks arising from them'.

The guidance is detailed and specific, in part owing to the more complex assessment of criminal liability under sections 45 and 46 of the Criminal

30 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf. The Criminal Finances Act, s.47(1), provides that the Chancellor of the Exchequer must prepare and publish guidance about procedures that relevant bodies can put in place to prevent persons acting in the capacity of an associated person from committing UK tax evasion facilitation offences or foreign tax evasion facilitation offences.

© Law Business Research 2021

Finances Act 2017, and because it builds on some of the more generic articulations of compliance guidance found elsewhere. For example, the articulation of commonly encountered risks from a tax fraud perspective is practical and useful as a starting point to prompt corporates and their advisers in their approach to risk assessment.

FCA Guidance – Financial Crime Guide and other sector-specific guidance 46.4.1.3

The various sources of FCA guidance are another useful tool in this field. A good starting point is Chapter 6 of the Senior Management Arrangements, Systems and Controls Sourcebook.[31] This provides 'organisational and systems and control requirements for all firms'. However, the principal detailed source of guidance the FCA provides on this is its Financial Crime Guide.[32] This comprehensive document draws on the FCA Financial Crime Thematic Reviews[33] to address risk in the specific areas of money laundering and terrorist financing, fraud, data security, bribery and corruption, sanctions and asset freezing, insider dealing and market manipulation.

The guidance is non-binding, but, where it is obviously appropriate for a corporate to address a particular risk, adherence to FCA guidance is likely to be beneficial generally and may be viewed favourably by UK law enforcement in the event of an investigation.

The thematic reviews are specific to certain business types, sizes or sectors, but are of more general assistance. Any corporate reviewing its compliance and procedures in a particular area of risk is likely to benefit from consulting any thematic review relevant to that risk area, even if its business does not sit in the reviewed sector.[34]

Another useful source of guidance for those responsible for compliance are the 'Dear CEO' warning letters the FCA issues with increasing frequency. For example, the FCA recently wrote to the chief executives of retail banks to share common themes arising out of its assessments of financial crime systems and controls within that sector.[35]

---

31 Compliance, Internal Audit and Financial Crime.

32 Financial Crime Guide: A firm's guide to countering financial crime risks (FCG).

33 Sixteen thematic reviews were conducted by the FCA between 2006 and 2014 resulting in 'general guidance' as defined in FSMA 2000, s.158.

34 For example, managing bribery and corruption risk in commercial insurance broking – update 2014 contains useful guidance about entering and managing third-party introducer relationships, which may be of assistance to corporates in other business sectors required to manage that risk.

35 Unsigned copy of a Dear CEO letter sent to Retail Banks (only) on 22 May 2021, 'Action needed in response to common control failings identified in anti-money laundering frameworks', https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-common-control-failings-identified-in-anti-money-laundering-frameworks.pdf.

© Law Business Research 2021

46.4.1.4 Joint Money Laundering Steering Group guidance

The Joint Money Laundering Steering Group (JMLSG) guidance[36] is aimed at firms operating under the auspices of the JMLSG's 14 UK trade association member bodies, in addition to those regulated by the FCA. It is approved by HM Treasury and therefore, relevant for the offences under the Proceeds of Crime Act 2002 (regulated sector) and Regulation 86 of the MLTF Regulations.

While it is not legally binding, firms 'will have to stand prepared to justify departures' from the guidance, which is split into three parts. Part I contains guidance relevant to all firms operating across the UK financial sector. Parts II and III provide additional sector-specific guidance.

The focal point of the JMLSG guidance is the responsibility of senior managers, including the money laundering reporting officer, to identify, assess and effectively manage money laundering risks across different aspects of their businesses. The JMLSG emphasises that there are many similarities between the strategies adopted by businesses to combat money laundering and other types of financial crime, such as fraud and market abuse, and recommends fostering 'strong links' between those responsible for managing and reporting on these various areas of risk.

The JMLSG guidance is clear that there is no one-size-fits-all approach and policies and procedures should be proportionate to the size and nature of the relevant business. There are strong parallels with the MOJ's six principles.

46.4.1.5 SFO Guidance on Evaluating a Compliance Programme

The SFO has published its internal guidance on how it will evaluate the effectiveness of an organisation's compliance programme.[37] This evaluation will be key in its determination whether a prosecution is in the public interest. Such assessment will be arranged around the MOJ's six principles, which the SFO recognises represent 'a good general framework for assessing compliance programmes'.[38]

In its guidance, the SFO recognises that appropriate compliance arrangements will vary, but states there is an expectation that all organisations, irrespective of size, will have at least some compliance arrangements in place. A compliance programme cannot be a 'paper exercise' and, to be effective, must be proportionate, risk-based and regularly reviewed.

The SFO does not state what it will consider adequate, having made clear previously that this is not its role. Each case will be assessed on its facts taking into account the company's risk profile and the steps taken to mitigate that risk.

Finally, the SFO states that in assessing an organisation's compliance programme it will look at the past (i.e. what was in place at the time of the

36 Prevention of money laundering/combating terrorist financing: guidance for the UK financial sector, June 2020 (amended July 2020).

37 SFO Operational Handbook: Evaluating a Compliance Programme (January 2020).

38 ibid., p. 5.

© Law Business Research 2021

alleged offence), the present and, where a DPA is being considered, the future. This emphasises the importance of commencing immediate remediation when potential criminal issues arise. Importantly, the SFO also foreshadows a move towards the use of corporate monitors stating that any DPA that includes terms relating to an organisation's compliance programme is 'likely to include a monitor being appointed at the organisation's expense'.[39]

Examples of US-based guidance 46.4.2

Joint SEC and DOJ Resource Guide 46.4.2.1

In July 2020 the Enforcement Division of the Securities and Exchange Commission (SEC) and the Criminal Division of the US Department of Justice (DOJ) produced an updated (from 2012) version of the Resource Guide to the US Foreign Corrupt Practices Act (FCPA),[40] describing it as 'one of the most thorough compilations of information about any criminal statute'.[41] Chapter 5 'Guiding Principles of Enforcement' includes sections on 'Hallmarks of Effective Compliance Programs' and 'Other Guidance on Compliance and International Best Practice'. Unsurprisingly, given the risk area under consideration, the Guide pays particular attention to 'Third Party Due Diligence and Payments' and offers three guiding principles when assessing due diligence in this area:

- *Identity*: A careful assessment of the identity of the third party; its qualifications and associations;
- *Rationale*: A clear understanding of a legitimate business rationale for the use of the third party in any piece of business it is involved in. This is likely to include information as to specificity of services, payment commensurate to the services undertaken, proof of work undertaken and payment terms and mechanisms which are regular and verifiable;
- *Ongoing Monitoring*: examples provided are periodic updating of due diligence, exercising audit rights, periodic training and annual compliance certification.

In addition to a worked-through hypothetical example involving third-party vetting, this Guide also directs corporates to the DOJ Criminal Division guidance on Evaluation of Corporate Compliance Programs, other US government departments' guidance and well-regarded international guidance such as that provided by the OECD and the World Bank.[42]

---

39 This was borne out in *SFO v. G4S Care & Justices Services (UK) Ltd*, Crown Court (Southwark), 17 July 2020, which was the second DPA to be agreed after the SFO published its guidance and saw the appointment of the first monitor under the DPA regime.

40 US Department of Justice and the US Securities and Exchange Commission, A Resource Guide to the US Foreign Corruption Practices Act, Second Edition, July 2020.

41 ibid., Foreword, page iii.

42 Working Group on Bribery, OECD, Good Practice on Internal Controls, Ethics and Compliance (February 2010); World Bank Group Integrity Compliance Guidelines (2017).

© Law Business Research 2021

46.4.2.2 US DOJ Criminal Division: Evaluation of Corporate Compliance Systems

This recently updated guidance issued by the DOJ's Criminal Division is another useful resource.[43] It sits as guidance across the whole of the division and is, therefore, applicable to other corporate offences as well as FCPA matters. It is more informative than the SFO's guidance, although the underlying principles significantly overlap. The DOJ guidance can also assist UK practitioners in discussions with the SFO about compliance-related issues in the course of DPA negotiations. The guidance comprehensively addresses how the DOJ will measure compliance programmes by reference to three key questions (sourced from the DOJ's Justice Manual) and is a useful reference for practitioners drafting or updating compliance programmes or considering potential outcomes and remediation in an investigation.

Is the programme well designed?

The DOJ will consider the quality of a company's risk assessment, policies and procedures, and training and communication; the existence and effectiveness of a confidential reporting mechanism; the application of risk-based due diligence to third-party relationships; and, where relevant, appropriate procedures to address mergers and acquisitions risk.

Is it being applied earnestly and in good faith?

The DOJ will focus on whether the compliance programme is well resourced and empowered to function effectively. This will entail a review of senior and middle management commitment and oversight; whether the compliance function can operate autonomously and with suitable resources; a comparison of the seniority and stature of the compliance function with other strategic functions within the company and the existence of incentives for compliance and disincentives for non-compliance.

Does it work in practice?

The DOJ will assess whether the programme has been periodically tested, reviewed and improved, including how the organisation measures its compliance culture. It will evaluate a company's investigations structure, its ability to conduct a root cause analysis of misconduct and whether root causes have been remedied in an appropriate and timely manner.

43 US Department of Justice, Evaluation of Corporate Compliance Programs (updated June 2020).

© Law Business Research 2021

US DOJ Antitrust Division: Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigation 46.4.2.3

This complementary guidance in the antitrust risk area poses the same three questions identified in the Criminal Division's Guidance and provides specific guidance looked at from context of 'criminal violations of the Sherman Act such as price fixing, bid rigging and market allocations'.[44]

DOJ FCPA Opinion Procedure 46.4.2.4

In addition to published guidance, the US system also affords companies the ability to request a formal opinion from the DOJ, as to whether a contemplated course of conduct will conform to its current enforcement policy under the FCPA. This mechanism is known as seeking an FCPA opinion.

The applicable regulations are clear that an FCPA opinion may only be sought in respect of 'prospective – not hypothetical – conduct'.[45] That is to say, 'the entire transaction which is the subject of the request must be an actual . . . transaction'.[46] While it may contain an element of historical conduct 'in most – if not all – instances, an Opinion request should be made prior to the requester's commitment' to proceeding with the transaction in question.[47]

FCPA opinions are available to 'issuers and domestic concerns', which includes individuals who are US citizens, nationals or residents and corporations and partnerships that have their principal place of business in the United States, or which are organised under US law.[48]

An affirmative FCPA opinion creates a rebuttable presumption in any subsequent action brought by the DOJ under the relevant provisions of the FCPA[49] that the requester's conduct, as specified in the request, is in conformity with the DOJ's enforcement policy and the relevant provisions of the FCPA.[50] Such a presumption may be rebutted by 'a preponderance of the evidence'[51] and does not 'bind or obligate' any agency other than the DOJ, nor does it alter the requester's accountancy obligations.[52]

The most recent opinion was issued on 14 August 2020[53] after a gap of nearly six years, which is the longest period of inactivity since the inception of the procedure in 1980. This gap raises issues as to the extent of the availability

44 US Department of Justice, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (July 2019).

45 28 C.F.R. part 80 (current as of 1 July 1999), § 80.1, Purpose.

46 ibid., § 80.3, Transaction.

47 ibid., § 80.3, Transaction.

48 ibid., § 80.4, Issuer or domestic concern and 15 USC § 78dd-2(h)(1).

49 15 U.S.C. §§ 78dd-1 and 78dd-2.

50 28 C.F.R. part 80 (current as of 1 July 1999), § 80.10.

51 Id.

52 ibid., §§ 80.11 and 12.

53 No. 20-01, 14 August 2020, Foreign Corrupt Practices Act Review Opinion Procedure Release.

© Law Business Research 2021

of opinions under the procedure and whether this potentially valuable procedure will be more frequently used in the future.

The DOJ confirmed that it would not bring enforcement proceedings in relation to a proposed fee of US$237,500 to be paid to a wholly owned subsidiary of a foreign investment bank by a multinational firm headquartered in the United States. Compliance and due diligence issues featured heavily in the rationale for the opinion. In granting the Opinion, the DOJ placed reliance on the identification of specific legitimate services in respect of the fee, the commercially reasonable and commensurate nature of the fee to the services rendered and the representations from the chief compliance officer of the entity receiving the payment that the monies will not be forwarded to any entity or individual or used to benefit any individual. This is a clear example of the Opinion Procedure in action and is likely to be of wider use to corporates, beyond the original corporate requester, seeking to understand how the guidance might apply to a set of facts under investigation.

46.5 The interplay between culture and effective compliance

The effectiveness of an organisation's compliance programme is intrinsically linked to its culture. This is recognised in the US Sentencing Guidelines Manual, which states that, to have an effective compliance and ethics programme, an organisation shall 'promote an organisational culture that encourages ethical conduct and a commitment to compliance with the law'.[54]

Culture, which is defined by the FCA as 'the habitual behaviours and mindsets that characterise an organisation',[55] significantly impacts compliance in several ways. It will influence whether compliance programmes are implemented and applied effectively; in the event of misconduct, it will have a bearing on the availability of a compliance-based defence to the company; and it will ultimately influence the type of resolution available to the organisation and the terms of that resolution.

The rule-based nature of compliance means that it is more likely that those rules will be ignored or circumvented where a defective organisational culture exists. The FCA has found that 'culture in financial services is widely accepted as a key root cause of the major conduct failings that have occurred within the industry in recent history'.[56] Similarly, failures in culture have been at the heart of many of the SFO's DPA resolutions where criticism has been made of corporates who have failed 'to instil within the wider business a culture of compliance'.[57] In some cases there has been a culture of pressure to meet targets[58] and in others a 'culture of wilful disregard of the commission

54 US Sentencing Guidelines Manual, chapter 8 (§ bB2.1) (2018).

55 FCA Discussion Paper DP 18/2: Transforming culture in financial services, March 2018, p. 3.

56 Id.

57 *Rolls-Royce* judgment, para. 102.

58 See *SFO v. Tesco Stores Ltd*, Crown Court (Southwark), Case No. U20170287 10 April 2017 (Statement of Facts, para. 55).

© Law Business Research 2021

of offences'[59] with the consequence that rules were ignored or internal and external compliance procedures deliberately circumvented.[60] In the case of Airline Services Ltd, the court noted that the company's senior management failed to implement an effective compliance programme, despite receiving a guide and recommendations.[61]

As is apparent from all the available guidance, even if misconduct does occur, an organisation that has fostered a culture of integrity is more likely to be successful in demonstrating the adequacy of its procedures, assuming it can evidence its efforts to do so.[62] The CPS prosecution of Skansen (the only contested adequate procedures case to date) is instructive in this regard. Skansen relied on its culture of honesty and integrity as part of its adequate procedures defence but faced evidential difficulties owing to its failure to document its attempts to implement compliance procedures and instil a culture of compliance.

Finally, culture is an important driver in the outcome of any investigation. Genuine attempts by a corporate to change its culture and focus on compliance are factors the court will consider when determining whether a DPA is in the interests of justice.[63] Effecting culture change is also key to remediation and ensuring that similar misconduct will not occur again. In the United States, cultural change is a common feature of compliance monitorships, and the DOJ has made plain that changes in culture, particularly where there has been a change in leadership, may be sufficient to guard against future misconduct and may avoid the need for a monitor at all.[64] This was the case for gold refinery Republic Metals Corporate (RMC) who entered into a non-prosecution agreement (NPA) with the DOJ in 2019 following an investigation into money laundering and violations of the Bank Secrecy Act. RMC avoided the imposition of a monitor with the DOJ citing its 'significant efforts to create a culture of proper compliance'.[65]

---

59 *Rolls-Royce* judgment, para. 104.

60 *Airbus* judgment, para. 65; *Amec Foster Wheeler* judgment, para. 24 ('The policies changed, but they never worked because FWEL [Foster Wheeler Energy Limited] did not want them to.') (*per* Edis LJ).

61 *Airline Services Ltd*, judgment, para. 49.

62 See, for example, Principle 2 of the Bribery Act guidance (pp. 23–24).

63 See *Sarclad*, preliminary judgment, para. 32.

64 See the Benczkowski Memo, 11 October 2018. 'Where misconduct occurred under different corporate leadership or within a compliance environment that no longer exists within a company, [prosecutors] should consider whether the changes in corporate culture and/or leadership are adequate to safeguard against a recurrence of misconduct.' A similar line of reasoning was applied in the UK DPA with Amec Foster Wheeler Energy Limited, where the SFO did 'not require that a monitor be installed in recognition of the substantial enhancements and modifications to the E&C Programme [multi-year, group wide ethics and compliance policies and procedures] and remediation exercise that have already been undertaken' (DPA, para. 44).

65 Non-Prosecution Agreement between DOJ and RMC, 8 March 2019.

© Law Business Research 2021

46.6 The impact of compliance on prosecutorial decision-making

The available guidance and resolutions to date demonstrate the correlation between effective compliance and the response of enforcement to address alleged corporate offending.

In its compliance guidance, the SFO is clear that its assessment of a corporate's compliance programme will be a critical consideration in determining whether (1) a prosecution is in the public interest, (2) the organisation should be invited into DPA negotiations, and what conditions the DPA should include, (3) the 'adequate procedures' defence is available in the case of a section 7 offence, and (4) it reflects greater or lesser culpability in terms of sentencing.

Similarly, in the United States, the joint DOJ/SEC Resource Guide to the US FCPA directs readers to the US Justice Manual: 'A prosecutor may also consider other remedial actions, such as improving an existing compliance program or disciplining wrongdoers, in determining whether to charge the corporation and how to resolve corporate criminal cases'.[66] The issue of the potential impact of a positive corporate culture is again reiterated here in the Justice Manual's comment; 'In determining whether or not to prosecute a corporation, the government may consider whether the corporation has taken meaningful remedial measures. A corporation's response to misconduct says much about its willingness to ensure that such misconduct does not recur.'[67]

Decision to prosecute

Compliance features in a number of ways in the decision to prosecute. The UK Guidance on Corporate Prosecutions states that it will be a public interest factor tending towards prosecution if, at the time of the alleged offence, an ineffective compliance programme was in place.[68] Conversely, the existence of a genuinely proactive and effective compliance programme will militate against prosecution. Prosecutors will also undertake a qualitative evaluation of steps taken by a corporate to remediate and enhance its compliance programme. The UK FCA, in its Enforcement Guidance, places similar emphasis on the ability of a firm to demonstrate that it has taken appropriate remedial action, such as addressing any systems and controls issues.[69]

In considering whether to prosecute failure-to-prevent offences, the prosecutor will evaluate whether an adequate procedures or reasonable procedures defence is available to the corporate and the likelihood of its success at trial.

Unlike the United Kingdom, the United States has a formal and public process of declinations that allows for agreed specific improvements to compliance processes, as well as other remediation terms (such as restitution and disgorgement) as factors on which the decision not to prosecute is based.

66 US Justice Manual § 9-28.1000(A), Restitution and Remediation.

67 US Justice Manual § 9-28.1000(B), Restitution and Remediation.

68 Crown Prosecution Service Guidance on Corporate Prosecutions.

69 The Enforcement Guide, FCA Handbook

© Law Business Research 2021

For example, the declination in respect of World Acceptance Corporation issued in August 2020 cited 'World's full remediation, including the additional FCPA training added to World's compliance program, separation from executives under whom the misconduct took place and discontinuing relationships with third parties in Mexico involved in the misconduct' as one of the five factors on which the decision was based.[70]

DPA considerations

Whether an organisation had an effective compliance programme is similarly relevant to deciding whether to invite a corporate to enter into a DPA, as is a corporate's ability to demonstrate that it has willingly taken remedial action to reform and rehabilitate. The likely terms of a DPA are also closely tied to this issue, in particular regarding the appointment of a monitor.

Paragraph 7.11 of the UK DPA Code of Practice[71] articulates the (sometimes delicate) balance involved in determining whether a monitorship will be appropriate.

> *An important consideration for entering into a DPA is whether [the corporate] already has a genuinely proactive and effective corporate compliance programme. The use of monitors should therefore be approached with care. The appointment of a monitor will depend upon the factual circumstances of each case and must always be fair, reasonable and proportionate.*

Therefore, at the time the terms of a DPA are agreed, a close analysis can be expected of specific remediation undertaken at that point, in the context of the corporate's overall compliance culture, to determine the most appropriate compliance-related terms of the DPA.

Determining financial penalty

The quality of a compliance programme is also relevant to the determination of any financial penalty, either as a term of a DPA or on sentencing, and will form part of the court's assessment of the corporate's culpability. In particular, in the United Kingdom for section 7 offences, evidence of a culture of wilful disregard to the commission of offences by employees or agents, with no effort to put effective preventative systems in place, will indicate high corporate culpability, while some effort to do so may indicate lesser culpability. The level of fine imposed may also be adjusted to avoid any negative impact on the company's ability to implement an effective compliance programme going forward.

---

70 US Department of Justice, Letter to Womble Bond Dickinson re World Acceptance Corporation, 5 August 2020.

71 SFO and CPS joint Deferred Prosecution Agreements Code of Practice (Crime and Courts Act 2013).

© Law Business Research 2021

46.7 Key compliance considerations from previous resolutions

In the United Kingdom, organisations can derive some assistance about what makes for effective compliance from concluded section 7 criminal investigations and FCA regulatory outcomes. However, this is an evolving area and, for example, what constitutes adequate procedures has not been properly tested. The only contested section 7 case is the successful CPS prosecution of *Skansen*, which provides little insight into the application of the statutory defence except for the importance of documenting compliance efforts. Furthermore, many investigations were resolved by DPA, meaning that the companies accepted that their procedures were not adequate, removing the need for the courts to test the issues.

In the United States, there is a more extensive body of declinations, DPAs and NPAs, in which the principles and guidance in respect of corporate compliance and due diligence have been put into effect.

The compliance deficiencies identified and explained in these cases assist in drawing the following lessons, applicable to all areas of legal risk.

- *Policies and procedures*: Should be carefully tailored to the corporate's individual risk profile in a specific area. This is a recurring theme in all of the guidance and the failure to do so, resulting in a failure to prevent the criminal risk, features in many of the DPA and final notice cases.
- *Compliance functions*: Should be independent, well resourced and empowered.
- *Independence*: Both Rolls-Royce and Airbus restructured their compliance units to ensure functional independence from the business including reorganisation of reporting lines. Similarly, Tesco plc[72] simplified reporting lines to ensure that there was clearer accountability and that those who had oversight of the business were independent from those that led it. Although these were steps taken by large multinational organisations, the principle has equal importance for small and medium-sized enterprises (SMEs), where fewer checks and balances tend to exist and a smaller group of individuals will control the business. Conversely, a failure to address this issue was a factor in the prosecution of Siemens in the United States in 2008. The information upon which Siemens' guilty plea was based cited an under-resourced corporate compliance function and 'an inherent conflict in its mandate, which included both defending the company against prosecutorial investigations and preventing and punishing compliance breaches'.[73]
- *Resourcing*: A common feature of remediation in the DPAs is the increase in compliance resourcing.[74] The DPAs indicate that SMEs can take a proportionate approach to resources and that the SFO and court will be willing to take into account size and means. For example, it was sufficient for SMEs Sarclad and Güralp Systems to undertake their DPA compliance reviews

72 See *Tesco*. This was not a section 7 case and Tesco Stores Ltd entered into a DPA in respect of one count of false accounting.

73 *USA v. Siemens Aktiengesellschaft*, Information, 12 December 2008.

74 See, for example, *Rolls-Royce*, *Tesco*, *Airbus*.

© Law Business Research 2021

internally[75] while listed companies Standard Bank and Tesco agreed to instruct leading accountancy firms as a term of their DPAs.

- *Empowerment*: In both the *Rolls-Royce* and *Airbus* UK DPAs compliance teams were not 'empowered to function effectively'[76] and, as a consequence concerns raised by compliance staff were ignored or overruled. For a compliance function to be empowered a true culture of compliance, led from the top, must be instilled. This will embrace the 'top level commitment' principle in the Bribery Act guidance. Empowerment will be easier to achieve if the compliance function is independent and well resourced.
- *Compliance functions*: Should be fully integrated across a group structure: Organisations must ensure that compliance procedures are applied across the group and that checks are in place to ensure that key processes are not overlooked. This is particularly important where complex multi-jurisdictional structures are involved. This issue arose in *Standard Bank*, in which two subsidiaries[77] of Standard Bank Group collaborated to raise funds on the debt capital markets for the government of Tanzania. Although both Standard Bank and Standard Bank Group had a number of committees, policies and procedures in place to prevent bribery, the SFO found the applicable policies to be unclear and not reinforced effectively through communication. Further, training had provided insufficient guidance about applicable anti-bribery obligations and procedures where two Standard Bank Group entities were involved in a transaction and one engaged an intermediary. A more sophisticated approach is likely to be required where multi-disciplinary compliance functions require integration by the corporate. In the US *Airbus* DPA, the statement of facts noted that one of the factors that had resulted in Airbus' violation of the ITAR (International Traffic in Arms Regulations) was 'the Company structuring the compliance function as separate and siloed from business sales and the export compliance function, which prevented accurate ITAR compliance'.[78]
- *M&A risk should be adequately assessed*: Where relevant, organisations should ensure that their compliance programmes address M&A activity. In *Sarclad*, Heico Companies LLC had acquired Sarclad in February 2000. While there is no suggestion of compliance failures on Heico's part,[79] it does raise the question what compliance steps Heico might take if the acquisition took place now. Pre-acquisition due diligence is a common feature of compliance

75 As a term of their DPAs, Sarclad's chief operating officer conducted a compliance review while Güralp Systems' compliance officer conducted a compliance review.

76 See US Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs guidance (updated June 2020), Section II.

77 Standard Bank and Stanbic Bank Tanzania Ltd.

78 *US v. Airbus* DPA, 31 January 2020.

79 The conduct that Sarclad accepted had taken place began some four years after acquisition in 2004 and the acquisition was at a time when compliance programmes were less developed generally and not subject to the same level of scrutiny as today.

© Law Business Research 2021

programmes but companies should also design processes for the full, effective and timely integration of compliance procedures post-acquisition.[80]

- *Intermediary relationships are very high risk*: Organisations should pay particular attention to compliance processes in respect of intermediaries. Eight of the nine section 7 DPAs[81] have involved intermediaries, and they also featured in the SFO's prosecution of *Alstom*.[82] By the time the court approved the *Rolls-Royce* DPA, the company had already addressed the potential risks arising from its use of intermediaries through the review of 250 such relationships across the organisation, resulting in the suspension of 88 intermediaries. In its final notice to *JLT Speciality Ltd*,[83] the FCA noted that an element of the breach of Principle 3 was that there was no separate assessment of risk in respect of each new piece of business introduced by the intermediary, meaning the company could not ensure it took sufficient steps to counter the risk of bribery and corruption. There should be ongoing scrutiny of any intermediary relationship, including whether it remains necessary, and a rigorous assessment of the compliance function that reviews it.
- *Act on warnings and learn from past mistakes*: A failure to act on early warnings or improve systems and controls following a previous incident may be an aggravating feature in determining outcome and penalty. This was the case for *SCB*, which did not act on AML weaknesses identified by Group Internal Audit, which may have prevented the breach. However, the *Rolls-Royce* UK DPA was approved by the court, notwithstanding criminal investigations in different countries that indicated the presence of these failures. The issue was relevant to the overall balancing exercise of whether a DPA was in the public interest, but on this occasion Rolls-Royce benefited from a DPA in any event.
- *Proactive self-assessment is beneficial*: Corporates should be prepared for an improved compliance programme to the surface current or historic issues and may require consideration of a self-report. This was the case for Heico when it integrated its compliance programme into Sarclad. For those organisations that do discover potential misconduct, it is apparent from an analysis of each DPA that it is less likely that an independent reviewer or monitor will be imposed where corporates have engaged in proactive remediation. Rolls-Royce and Airbus had each retained and acted on the recommendations of an independent reviewer prior to the court's consideration of the

80 The DOJ Compliance Guidance is helpful on this point.

81 Those agreed between the SFO and Standard Bank, Sarclad, Rolls-Royce, Airbus, Airline Services Limited, Amec Foster Wheeler, and AB Ltd and CD Ltd.

82 *R v. Alstom Network UK Ltd* [2019] EWCA Crim 1318. A pre-Bribery Act prosecution that concluded in November 2019 with Alstom Power Ltd having pleaded guilty to one count of conspiracy to corrupt and Alstom Network UK Ltd having been convicted of a further count of conspiracy to corrupt.

83 Final Notice, 19 December 2013.

© Law Business Research 2021

terms of their DPAs. Equally, the Serco Group[84] had implemented a comprehensive corporate renewal programme. As a term of their DPAs, Rolls-Royce and Airbus were allowed to continue with their choice of independent reviewer, and the Serco Group was given responsibility for the review of its own group-wide compliance programme. However, this should be contrasted with the outcome for G4S who, despite extensive remediation, had stringent compliance conditions imposed as a term of its DPA, including the appointment of an SFO-approved reviewer at the company's expense. This appointment constitutes the closest the SFO has come to requiring the appointment of a US-style monitor to date. Conversely, any corporate that fails to identify its failings in this area, or worse, fails to respond adequately to intervention by law enforcement or regulators should expect a more severe outcome in the event of prosecution or regulatory action. For example, the final notice issued to Besso Ltd[85] for breaches of Principle 3 identified a failure to take sufficient or timely steps to remedy shortcomings in its bribery and corruption risk systems and controls after two visits from the FCA to inspect them as an aggravating feature. In the United States, where declination is available to law enforcement, the benefits of proactive self-assessment may be even greater. Invariably, the DOJ FCPA declinations cite 'the steps that the Company has taken to enhance its compliance program and its internal accounting controls' as a factor contributing to the decision not to prosecute.[86]

See Chapter 33 on monitorships

- *A comprehensive documentary record of all compliance processes is essential and promotes good practice*: From an investigations perspective, a solid evidential basis for defending potential enforcement action is critical. A good quality record of the implementation of compliance processes is likely to be the best evidence of this.

Conclusion 46.8

Effective compliance is critical to mitigating the risk of financial crime or misconduct within organisations. While compliance programmes cannot prevent isolated incidents of misconduct, an organisation that has sought to implement robust, risk-appropriate compliance procedures stands a better chance of demonstrating the sufficiency of those procedures and securing a favourable outcome, particularly where it is has done so in the context of a positive culture of corporate integrity. In the event of a suspected breach, as part of the investigation, corporates should be ready to evidence a proportionate and risk-based approach to compliance, driven by senior management, where risk assessments and procedures have been regularly reviewed, staff are adequately trained and the procedures have been fully and properly implemented.

84 *SFO v. Serco Geografix Ltd*, Crown Court (Southwark), 4 July 2019 Case No. U20190413. Serco Geografix Ltd entered into a DPA in respect of five counts of fraud and false accounting.

85 Final Notice, 17 March 2014.

86 See, for example, US Department of Justice Criminal Division, Letter to K&L Gates dated 3 June 2016 in respect of Nortek, Inc.

© Law Business Research 2021

47

Environmental, Social and Governance Investigations

Emily Goddard, Anna Kirkpatrick and Ellen Lake[1]

Introduction 47.1

Investigations relating to environmental, social or governance issues are not new. However, over the last decade the interest in 'ESG'– a term thought to have been coined by a 2005 UN Global Compact study[2] – has grown and ESG factors have become important criteria for investors to identify material risks and, increasingly, growth opportunities. With more attention on the risk and rewards, ESG-related investigations are on the rise. These are now often led by lawyers because of the growing legal and regulatory implications, and the sensitivities frequently involved. We look at some common features and challenges of investigating these issues, and how these can be approached in effective ESG-related investigations.

ESG issues and investigation triggers 47.2

Over a number of years ESG has fast risen to the top of board agenda, with companies more aware that failure to address these matters can be detrimental to their businesses legally, financially, operationally and reputationally. Global events such as #MeToo, Black Lives Matter and increased climate change activism have turned the spotlight onto ESG practices such as whistleblowing

1 Emily Goddard is an associate and Anna Kirkpatrick and Ellen Lake are senior associates at Clifford Chance. The authors would like to thank their colleagues Amy Bird, Michael Coxall and Michelle Williams for their assistance in preparing this chapter.

2 The Global Compact, 'Who Cares Wins: Connecting Financial Markets to a Changing World' (2004). In 2006, the concept of ESG was integrated into the UN-backed Principles for Responsible Investment, which provide a framework for the incorporation of ESG factors into investment practice.

© Law Business Research 2021

See Chapters 19 and 20 on whistleblowers

arrangements, diversity and inclusion, and environmental crisis management. ESG issues have gained traction in global policy discussions, an example being the UN Climate Change Conference (COP26) that took place in November 2021, with a focus on ESG reporting as a driver of positive change. Investors and investment managers, among other stakeholders, look to ESG criteria to assess whether businesses are attractive propositions and the level of ESG risk they carry, and there is growing external pressure from governments, regulators and international organisations to do so. Business leaders are increasingly accepting the need to proactively identify their own ESG standards, against which stakeholders will hold them to account. Building compliance frameworks to meet those expectations and considering response plans are just some of the ways that companies can mitigate ESG risk.

But what are ESG issues and when do investigations into them arise? What falls within ESG is evolving, and the intersectionality between the three pillars makes division into individual concepts artificial, but broadly:

- *Environmental*: Fuelled by media coverage, there is increasing pressure on companies to take responsibility for their role in environmental impacts. The environmental criteria by which a company might be judged include its use of energy, how it uses raw materials and deals with its waste, and how it interacts with the natural world. There is progressively more law and regulation being made in this area, including mandatory reporting obligations. Businesses are responding to these obligations and to activist investors by setting climate change targets against which they can be held to account. An ESG-related environmental investigation can differ from a 'traditional' environmental investigation[3] as the focus is not only on scientific and technical assessments of root cause and impact, but also on the company's potential culpability, its actions and what can be inferred about its governance.
- *Social*: Social criteria typically look at the impact businesses have on society and how companies remedy harms they cause or contribute to, with an emphasis on transparency of communication. To meet stakeholder expectations, companies are seeking to demonstrate that they have a positive impact on the people and communities with whom they have a relationship. Conversely, it is increasingly clear that companies can face serious reputational damage, financial loss, operational disruption and legal liability if they are involved in human rights abuses, for example, through their supply chain. As a result, a number of businesses are attempting to reduce harm and negative impacts on people and their rights. Moreover, companies' positive and negative impacts are increasingly being assessed, including through

3 See, for example, BP's investigation into the Deepwater Horizon matter in 2010. The technical report by BP's internal incident team was made publicly available: 'Deepwater Horizon, Accident Investigation Report' (8 September 2010), https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/sustainability/issue-briefings/deepwater-horizon-accident-investigation-report.pdf.

© Law Business Research 2021

mandatory reporting to regulators and voluntary reporting to ESG rating organisations, on workplace behaviours and culture, diversity and inclusion of the workforce, and the accountability of executives.

- *Governance*: Governance factors determine, for example, how a business is controlled and overseen by its board and senior management, assesses and manages its risks, makes decisions, obtains and acts on staff feedback, remediates shortcomings and is structured. When considering ESG issues, environmental and social factors such as climate change or human rights risks stand out more prominently. However, corporate governance is often significant in determining how successfully a company fulfils its environmental and social responsibilities. It may have a bearing on whether incidents occur and, if they do, on how effectively they are investigated and remediated. 'Good' governance factors can range from accurate and transparent company reporting, to employee engagement (including grievance and collective consultation mechanisms, and whistleblowing arrangements). Allegations of poor corporate governance have underpinned a number of high-profile ESG failings.[4] Poor governance can also result in or amplify the effect of bribery and corruption failings or failings in a business's supply chain, among other things.

Against this backdrop, there are a multitude of potential triggers for investigation – both internal and external. Salient examples include the following:

- *Environmental disasters*: Events such as an oil spill or the collapse of a dam can trigger investigations into the adequacy of the risk management processes put in place by businesses to prevent them.
- *Supply chain issues*: The complexity and global nature of supply chains render them vulnerable to bribery and corruption and human rights abuses that often entail labour abuses, but can also include negative impacts on other human rights, including the rights related to health, food, land or water.[5]
- *Displacement of communities*: Many large-scale infrastructure projects lead to the displacement of communities. The social impact can be severe and can trigger huge pressure from non-governmental organisations (NGOs) and others to conduct investigations.
- *Discrimination, harassment and culture*: Alleged incidents of workplace misconduct continue to trigger investigations. Poor culture in all or part

4 See, for example, the multiple investigations into Volkswagen's emissions testing, 'Volkswagen to sue former management over Dieselgate' (26 March 2021), https://globalinvestigationsreview.com/fraud/german-car-manufacturer-volkswagen-will-take-legal-action-against-its-former-ceo-and-the-head-of-its-audi-unit-over-alleged-negligence-linked-the-long-running-and-costly-diesel-emissions-scandal.

5 See, for example, recent allegations of forced labour use at supplier factories, 'BooHoo to launch investigations into its supply chains: Independent Review into the boohoo Group PLC's Leicester supply chain' (24 September 2020) https://www.boohooplc.com/sites/boohoo-corp/files/final-report-open-version-24.9.2020.pdf.

© Law Business Research 2021

of the business, including where employees feel unable to speak up, can manifest itself in many ways, such as in discriminatory behaviour[6] or sexual harassment allegations.[7] For regulated entities in the financial sector, non-financial misconduct (and more broadly, a non-inclusive culture or environment) is increasingly seen as a falling within the regulatory perimeter.

- *Greenwashing*: Investigations are beginning to arise from allegations of greenwashing, namely the misselling or misstatement of the sustainability credentials of a company or its financial products or performance (and, similarly, an emerging trend in relation to concerns over 'social washing'). This has been the subject of growing scrutiny by regulators. The UK Financial Conduct Authority (FCA) recently published a set of guiding principles to address greenwashing in ESG and sustainable investment funds.[8] The US Securities and Exchange Commission (SEC) recently formed a task force to proactively identify misstatements in ESG disclosures by public companies and investment managers.[9] SEC Chairman Gary Gensler has voiced specific concern about investment funds that market themselves as green or sustainable without using consistent data and criteria to substantiate these claims.[10] Unsubstantiated claims regarding the nature of ESG-focused funds also interest regulators because many charge substantially more in fees and other costs than non-ESG funds.

47.3 The legal and regulatory frameworks

As with any investigation, a key step is ascertaining the standards against which the subject matter will be assessed. These can be particularly complex in the ESG sphere. While there will be clear legal obligations engaged in some investigations, in others, companies may need to look at both 'soft' and 'hard' law commitments. Although not legally binding, soft law is typically prominent in the design and execution of ESG-related investigations, as companies seek to demonstrate not only strict compliance with law or regulation, but

6 See, for example, the investigation by the United Kingdom's Conservative Party following high-profile allegations of Islamophobia, 'Report of the independent investigation into alleged discrimination, citing protected characteristics, within the conservative and unionist party in England, Wales and Northern Ireland' https://singhinvestigation.co.uk/.

7 See, for example, the high-profile investigation into alleged misconduct of the CEO of UK fashion retailer Ted Baker, https://markets.ft.com/data/announce/detail?dockey=1323-14036908-6QQK7UD9OP59VBEI1KK552QP46

8 FCA Dear Chair letter, 'Authorised ESG & Sustainable Investment Funds: improving quality and clarity' (19 July 2021), https://www.fca.org.uk/publication/correspondence/dear-chair-letter-authorised-esg-sustainable-investment-funds.pdf.

9 SEC press release, 'SEC Announces Enforcement Task Force Focused on Climate and ESG Issues' (4 March 2021), https://www.sec.gov/news/press-release/2021-42.

10 Public Statement by SEC Chairman Gary Gensler in Prepared Remarks Before the SEC's Asset Management Advisory Committee (7 July 2021), https://www.sec.gov/news/public-statement/gensler-amac-2021-07-07.

© Law Business Research 2021

also transparency and a more comprehensive understanding of ESG issues. Any internal standards (including corporate policies and procedures), along with the company's external statements and disclosures, may also be relevant benchmarks against which investigations can be conducted (and reputational management may need to be employed).

In some areas, such as human rights, there is a relatively advanced framework against which to assess conduct – and against which knowledgeable stakeholders will expect a company to assess conduct. In other areas, the applicable standards will be less clear: the company will need to come to a view on what frameworks it will apply, while considering the likely expectations of stakeholders as to the appropriate standards (particularly where corporate standards have been publicly expressed). This lack of clarity, and the potential for a mismatch in expectations of relevant standards, makes ESG-related investigations particularly challenging.

Hard law 47.3.1

A vast amount of domestic legislation and regulation has underpinned each of the ESG pillars for several decades. For example, the broad frameworks underpinning environmental protection in the United Kingdom are well established.[11]

Further legislation and regulation focused on corporate involvement in ESG issues has been developing on both sides of the Atlantic. In the United Kingdom, this includes a duty on directors to promote the success of the company, including by having regard to a series of factors promoting ESG objectives.[12] In the United States, regulations are used at the federal level, but also at the state level, such as the Californian legislation requiring companies to disclose the extent of their due diligence with respect to human trafficking and slavery in their supply chains.[13]

As regulators respond to investor and consumer concerns, a number of additional legally binding obligations have been or are expected to be implemented, including individual accountability regimes, such as the Senior Managers and Certification Regime for certain regulated entities in the United Kingdom, under which the regulator expects 'firms to have clear roles and responsibilities for the board and its relevant sub-committees in managing the risk from

11 In the United Kingdom, environmental legislation is constantly being amended, updated and consolidated, but current examples include the Environmental Protection Act 1990 and Environmental Permitting (England and Wales) Regulations 2016.

12 Companies Act 2006, s.172.

13 The California Transparency in Supply Chains Act.

© Law Business Research 2021

climate change'.[14] Particularly notable are the increasing reporting, disclosure and due diligence requirements, for example:

- the EU Taxonomy Regulation[15] and Sustainable Finance Disclosure Regulation[16] require disclosure by qualifying entities on the environmental sustainability of their activities. Following Brexit, the United Kingdom intends to implement its own 'green taxonomy' and Sustainability Disclosure Requirements, mainly targeted at financial services firms and their investment products, requiring them to report on their impact on the climate and environment;[17]
- amendments to the SEC's Regulation S-K in August 2020 required all US public companies to include a disclosure topic in quarterly and annual reports describing each company's human capital resources to the extent that such disclosures are material to understanding the registrant's business; and
- the SEC recently requested comment on mandating additional ESG disclosures for public companies in their quarterly and annual reports; most responders strongly supported mandatory disclosure requirements and the SEC is working on proposed disclosure rules.

These requirements may be relevant both to assessment of the issues being investigated (i.e., failure to properly disclose on ESG matters) and to the conduct of the investigation itself (it may be appropriate or necessary to report on the decision, progress or outcome of any ESG-related investigation under the applicable rules). While climate change-related reporting requirements are generally the most advanced, companies should also be aware of other potentially relevant reporting requirements, such as money laundering reporting obligations or those relating to modern slavery.

47.3.2 Soft law

Soft law standards and principles provide a framework for companies seeking to advance their ESG credentials. There are two broad categories that are most likely to be relevant when conducting an ESG-related investigation:

14 Prudential Regulation Authority, Supervisory Statement SS3/19, 'Enhancing banks' and insurers' approaches to managing the financial risks from climate change' (April 2019), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2019/ss319.

15 Regulation (EU) 2020/852 (Taxonomy) on the establishment of a framework to facilitate sustainable investment.

16 Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector.

17 HM Treasury, 'Chancellor sets out how UK financial services can create prosperity at home and project values abroad in first Mansion House speech' (1 July 2021), https://www.gov.uk/government/news/chancellor-sets-out-how-uk-financial-services-can-create-prosperity-at-home-and-project-values-abroad-in-first-mansion-house-speech.

© Law Business Research 2021

consensus-based international standards and principles, and voluntary standards and principles.

International standards and principles 47.3.2.1

The most notable of the consensus-based international standards and principles are the UN Guiding Principles on Business and Human Rights (UNGPs). The UNGPs detail processes known collectively as human rights due diligence, which involves a company taking steps to identify, prevent, mitigate and account for how it addresses its potential or actual adverse human rights impacts, as well as processes to enable remediation of such impacts that occur where the company has caused or contributed to them. These processes have been applied beyond human rights, being incorporated in the OECD Guidelines for Multinational Enterprises (OECD Guidelines), for example, which prescribe a due diligence approach applicable in all areas where businesses can be expected to act responsibly (for example, the environment). Those carrying out ESG-related investigations increasingly consider whether the key precepts of the UNGPs and OECD Guidelines have been met in the conduct being investigated.

Further, the International Financial Reporting Standards Foundation's global ESG reporting standard, to be published in 2022, will be set by the new International Sustainability Standards Board, with its scope, format and content to be determined.[18] Ultimately the standards will need to be adopted in domestic law by jurisdictions or be a voluntary standard that companies adhere to alongside any mandatory regulatory reporting.

Voluntary standards and principles 47.3.2.2

Prominent voluntary ESG regimes at an international level include the Sustainability Accounting Standards Board and the Global Reporting Initiative. The latter is an independent organisation based in the Netherlands aiming to provide a common language for organisations seeking to communicate their ESG impacts. It creates accountability by allowing investors to see whether companies are enacting environmental conduct standards. Companies volunteer to be held accountable to evidence their good ESG practices.

Specific jurisdictional standards and principles, such as the UK Corporate Governance Code, may also apply. The FCA requires all companies with a UK premium equity shares listing to annually report on their application of the Code – on a 'comply or explain' basis, which includes setting out where they have not applied it – effectively making it part of company law for those entities. Private companies are encouraged to apply the Code, but do not have the same reporting requirement.

18 See the International Financial Reporting Standards's Sustainability-related Reporting website for current status, at https://www.ifrs.org/projects/work-plan/sustainability-reporting/#current-stage.

© Law Business Research 2021

ESG-related voluntary standards and principles can also be industry or sector-specific. For example, there are several financial sector voluntary initiatives, such as the Equator Principles, UN Environment Programme Finance Initiative/UN Global Compact Principles for Responsible Banking and UN Principles for Responsible Investing for investment managers and other investors. Similarly, the extractives industry is encouraged to look to standards including The Extractive Industries Transparency Initiative, The Responsible Gold Mining Principles and The International Council on Mining & Metals 10 Sustainable Development Principles. In some situations, companies will need to apply standards and principles as part of a commercial relationship; for example, clients of the International Finance Corporation (IFC) are required to uphold the IFC Performance Standards.

Companies subject to an ESG-related investigation should ensure any voluntary standards and principles that they claim to follow are adhered to in the investigation or the assessment, to protect the integrity of their ESG commitments.

47.3.3 Corporate standards

In addition to hard and soft law obligations, corporate standards – policies, procedures, codes of conduct and values – are essential benchmarks for an ESG-related investigation. This is particularly the case where a company makes public its ESG commitments, indicating to stakeholders that these are the standards against which it will hold itself, its employees and its business partners accountable. An ESG-related investigation will frequently find that corporate standards, and systems and controls to meet them, are part of the problem. In all ESG-related investigations, but particularly those where governance is found lacking, there is likely to be the need to feed back into the business the conclusions of the investigation and actions for putting in place more robust corporate standards – and ensuring compliance with and effective monitoring of those standards – to address investigation findings.

47.4 Particularities of ESG-related investigations

The traditional investigation considerations as to the scope, claims to privilege, resourcing, available expertise, governance, engagement with relevant regulators and law enforcement, engagement with stakeholders, etc., also apply in ESG-related investigations. However, a number of other issues arise owing to the often particular nature of ESG issues; we set out below some observations, and the common features and challenges.

47.4.1 Triggers

See Chapter 2 on risk management

Many of the triggers for ESG investigations, such as customer complaints, employees escalating concerns, employee surveys, whistleblowing reports, reviews by internal compliance or audit functions, or questions from regulators are common in any investigation. However, in ESG-related investigations,

© Law Business Research 2021

the range of stakeholders almost always extends further, and the ways issues can come to the fore are generally more varied. Numerous NGOs, consumer and employee groups, and the media have been actively exposing companies on ESG matters for some years, and investors, regulators, governments and policymakers now frequently join those stakeholders in applying pressure on companies facing ESG issues. Triggers may include enquiries by NGOs, internal leaks to NGOs or the press, and political pressure. These triggers are less easy to predict and monitor, and companies may find themselves more at risk of being blindsided by the discovery of an ESG issue and under more pressure to provide a response.

In such circumstances, companies should ensure that they counter this with an effective communications strategy at an early stage. This may be part of a wider crisis management strategy in the context of significant matters – but in almost all ESG-related circumstances will be relevant. Scoping is always important in the management of any investigation, but the scrutiny will likely be greater when considering whether it is appropriate for the company to investigate a particular ESG incident, or to undertake a wider investigation (for example, where a harassment incident indicates a more systemic cultural problem). An ill-advised press release that overpromises on the investigation may cause the company to lose control of the scope and set it up to disappoint stakeholders from the outset.

See Chapters 38 and 39 on publicity

Investigator expertise and independence 47.4.2

The many and varied stakeholders involved in ESG-related investigations may take a keen interest in not only the outcome and findings of the investigation but also its approach and conduct.

ESG expertise is growing within companies, but for those lacking the resources of large institutions, it may be necessary to bring in specialists in the ESG issues at play alongside others experienced in conducting investigations. Inadequate expertise or insufficient resources will undermine the investigation's credibility.

Independence can be particularly important in the context of ESG investigations, which often deal with sensitive issues, and any real or perceived conflict of interest may cast doubt on the investigation's integrity. Different degrees of independence may be implemented, from conducting the investigation internally with external legal advice, to instructing external counsel or another third party to lead the investigation. Whatever the approach, companies should be cautious in responding in the immediate aftermath of an ESG incident with a press release announcing a fully independent investigation. A stakeholder's interpretation of 'independent' in this context might translate as an expectation that the investigation will be wholly conducted by a third party with no existing relationship, or likely future relationship, with the company or its investors. Where this is not case (for example, when the investigation is

© Law Business Research 2021

a collaboration between the company and its external counsel),[19] it is important to be clear about the approach to 'independence' to avoid misleading engaged stakeholders.

47.4.3 Transparency, privilege and reporting

Companies may face pressure to be transparent about processes and their effectiveness, to ensure accountability. There could be tensions between these considerations and legal risks for the business. Companies will often make – and be expected by stakeholders to make – transparency commitments, which might include, in the context of an ESG-related investigation, the publication of some forms of investigation findings, such as a written report. Transparency commitments may also be enshrined in law, with some jurisdictions requiring some level of reporting on non-financial issues.

This may have implications for the company's ability to claim legal privilege over documents produced as part of the investigation. A company intending to have the benefit of legal privilege (or, in some jurisdictions, professional secrecy) will need to set up the investigation team according to the requirements of the relevant jurisdictions. However, while for internal investigations there are usually alternatives to publishing formal reports in order not to waive privilege (such as providing oral updates on factual findings), this may not be sufficient to adequately respond to the various stakeholders in an ESG investigation, who may expect a written report. Companies often make reports on ESG issues publicly available as a result.[20] Companies will want to consider this at the outset of any investigation and not assume that materials produced along the way will necessarily be withheld from publication at a later stage.

See Chapters 36 and 37 on privilege

47.4.4 Stakeholder engagement

Traditional investigations tend to be inward-looking and largely focus on the conduct and the consequential risks to the company. They often involve determining whether breaches or failings have occurred and identifying responsible parties. ESG-related investigations focus not only on business risk, but also on risk to external parties affected by the conduct under investigation. Where there are external 'rights-holders',[21] this will likely mean more engagement with potential victims, local communities, NGOs and others whose rights may be affected by, or who speak for those affected by, the relevant issues.

ESG investigations can touch on matters that mean that stakeholder engagement can be very challenging. Investigations looking at possible infringements

19 This is usually an effective approach, through the combination of external counsel's expertise, and internal personnel's familiarity with the company's business and internal standards.

20 See, for example, the BooHoo investigation, supra note 5.

21 Under the Universal Declaration of Human Rights, all human beings are 'rights-holders'; individuals are rights holders that can make claims, and states and other actors are 'duty bearers' that are responsible and can be held accountable for their acts or omissions.

© Law Business Research 2021

of human rights or environmental disasters will involve dealing with potential victims and often whole communities deeply and personally affected. Political tensions might also arise; for example, state-sponsored human rights abuses (e.g., in relation to forced labour) mean that a company with operations in certain jurisdictions can be at risk if it does not navigate an investigation carefully. Given these sensitivities, stakeholder engagement is a touchstone for each step of an ESG investigation. Engagement should be built into the investigation plan, and extensive interaction with external stakeholders such as rights holders and NGOs may be required.

Companies also need to understand that the existence of readily identifiable victims, rights holders and whistleblowers can change the dynamics of the investigation, and this frequently occurs in ESG investigations. Their rights will need to be carefully handled during the investigation, including in interviews. This may involve a balancing of requests for anonymity and data protection issues against the need to put allegations to implicated parties and report to stakeholders.

See Chapters 19 and 20 on whistleblowers

See Chapter 40 on data protection in investigations

Heightened business risk 47.4.5

Most traditional investigations will carry reputational, financial, operational and legal risk for the company. ESG-related investigations are no different, but typically those risks can be easily heightened.

- *Reputational risk*: An ESG investigation that is not properly handled can result in a reputation built up over many years disappearing overnight. Investors and wider society increasingly expect ESG factors to be taken into account by companies to guide governance, decision-making and strategy as part of responsible business conduct. Recent years have seen a rise in activist shareholders proposing or supporting resolutions requiring companies to adopt gold standards on ESG issues, or pushing for changes in corporate governance, as well as publishing score cards comparing companies' ESG performance. These actions are often supported by consumers and NGOs, who may also call for boycotts, generate negative publicity through campaigning on ESG issues, or put pressure on regulators to intervene and investigate allegations of ESG failures.
- *Financial risk*: As investors increasingly focus on, and publicly commit to, evaluating their holdings based on ESG criteria, failure to properly investigate and remediate ESG issues can lead to investors considering or opting to withdraw funding, resulting in loss of market capitalisation and access to capital. This is illustrated, for example, by Unilever's public statement that its approach of integrating human rights and other sustainability

© Law Business Research 2021

considerations into mergers and acquisitions made it an attractive buyer that might be differentiated among bids.[22]

- *Operational risk*: Clearly, ESG incidents can lead to business interruption for the company or to its supply chains. Where a misconducted investigation further damages a company's relationships with stakeholders, such as local communities, this may, for example, have implications for local recruitment, or amplify the risk that groups take actions to interrupt company business.
- *Legal risk*: While follow-on litigation and regulatory enforcement is a very real risk following many investigations, ESG issues attract a lot of attention. Increasing political and societal interest means additional prominence of ESG incidents in the media; there has been a rise in shareholder activism and NGO use of litigation to seek corporate accountability;[23] claimant firms and funders are active in the space; and regulators will likely feel they need to be seen to be taking action. To take climate change as an example, in recent years shareholders have pursued claims for failure to adequately report climate change risks, as well as for breach of directors' fiduciary duties to take the risks seriously in their decision-making. NGOs bring strategic claims for ESG failures, as well as supporting alleged victims in bringing claims. Businesses have faced increasing litigation in respect of non-financial misconduct, in particular sexual harassment allegations in the wake of #MeToo and Black Lives Matter. Increased claims by employee whistleblowers alleging that they have been subjected to a detriment or dismissal as a result of an ESG-type disclosure (for example, that a company is greenwashing products) are anticipated. Key to mitigating legal

22 Unilever Human Rights Progress Report 2017, p. 12, https://www.unilever.com/Images/human-rights-progress-report_tcm244-513973_en.pdf. 'Our approach to both environmental and social sustainability makes us an attractive buyer to many companies/shareholders who share our values and can be an important differentiator in a field of bidders.'

23 See, for example, *Vedanta Resources PLC and another v. Lungowe and Others* [2019] UKSC 20 (regarding alleged toxic emissions from the Nchanga Copper Mine in Zambia. The claimants are a group of 1,826 Zambian citizens alleging that both their health and their farming activities have been damaged by repeated discharges of toxic matter from the copper mine into their water sources from 2005 to date); *Mariana & Others v. BHP Group PLC and another* [2021] EWCA Civ 1156 (the Court of Appeal granted the applicants permission to appeal against the High Court decision in relation to a claim arising from the collapse of a Brazilian dam in 2015. The claimant group is made up of at least 200,000 people); *Milieudefensie et al v. Shell* [Hague District Court, Judgment of 29 January 2021 C/09/365498 / HA ZA 10-1677 (zaak a) + C/09/330891 / HA ZA 09-0579] (the Court found in favour of four Nigerian farmers and a number of environmental activists following six pipeline leaks in Nigeria. Shell's Nigerian subsidiary and the parent company, Royal Dutch Shell, were found to have violated their duty of care); and *Okpabi and others v. Royal Dutch Shell Plc and another* [2021] UKSC 3 (the UK Supreme Court concluded that it was at least arguable that the parent company owed a duty of care to the claimant Nigerian citizens in respect of alleged environmental damage and human rights abuses arising from oil leaks from pipelines and associated infrastructure operated by Shell's Nigerian subsidiary).

© Law Business Research 2021

risk is to consider it from the outset of the investigation, including awareness that the content of the investigation might feed, and be disclosed in, claims or enforcement actions in the future. Clear boundaries on the information produced and to whom it is circulated during the investigation will assist in containing material produced, as will communications protocols giving those privy to relevant information guidance on what communications are and are not appropriate.

See Chapters 5 and 6 on beginning an internal investigation and Chapters 38 and 39 on publicity

While control over the external environment to mitigate the risk is more difficult, companies can take proactive steps in advance of an incident occurring to encourage employees to raise issues internally before they escalate into business risk or are leaked to shareholders, the media or NGOs: promoting a strong internal 'speak up' culture; having efficient grievance and whistleblowing processes; engaging with staff at all levels; monitoring the effectiveness and outcomes of grievance processes; and appointing a non-executive or supervisory director with responsibility for engagement on these issues. Once the investigation is in progress, regular engagement with stakeholders will be important to try to minimise any dissatisfaction with the outcome and the likelihood of stakeholders seeking redress through the courts.

Remediation 47.4.6

It is important from a governance and stakeholder engagement perspective to track recommendations and actions arising as the investigation progresses. But consideration of remediation is not something that can be left to the end of an ESG-related investigation. While remediation follows many investigations, the sensitivity and high-profile nature of ESG issues mean that there will likely be a very strong expectation that an ESG-related investigation considers remediation as part of its recommendations, and so the thinking on remediation will need to be progressed alongside the investigation. This is particularly the case with societal issues, where frameworks such as the UNGPs require businesses to offer or participate in remediation where they have caused or contributed to adverse human rights impacts. Under such frameworks, whether or not businesses have caused or contributed to negative impacts, they are expected to design and implement grievance mechanisms and reporting channels to facilitate prompt and effective identification and resolution of potential future issues, as well as mechanisms to evaluate their own performance in this regard. In some cases, remediation may include disciplinary sanctions, which must be handled sensitively and appropriately to balance appropriate investigatory action with employment law requirements to mitigate future risk.

Some ESG issues may not be quickly remedied, and statements around remediation need to be realistic; failure to act on remediation commitments could result in further scrutiny or criticism. Similarly, remediation may require actions by third parties (for example, within the supply chain), where practicalities and contractual arrangements may hinder swift remediation.

© Law Business Research 2021

Appendix 1

About the Authors of Volume I

Ama A Adams
Ropes & Gray LLP

Ama A Adams is a litigation and government enforcement partner at Ropes & Gray in Washington, DC. Her practice focuses on international transactions and the US government's regulation of trade and investment. This includes, most notably, export controls, economic sanctions, anti-corruption, foreign direct investment and customs laws and regulations. In addition to advising clients on the application of international trade regulations to their business operations, Ms Adams also assists clients in developing compliance programmes, handling pre- and post-acquisition due diligence, conducting internal investigations relating to potential violations of trade laws and representing clients before the US government agencies in connection with enforcement matters and government inquiries. She advises companies in a range of industries, including the oil and gas, aviation, pharmaceutical, manufacturing, technology, chemical and financial sectors.

Stuart Alford QC
Latham & Watkins

Stuart Alford QC is a partner in the London office of Latham & Watkins, and a member and former co-chair of the firm's litigation and trial department in London. Mr Alford advises leading corporations, high-growth companies, and financial institutions in a range of financial crime and regulatory matters, particularly corruption, money laundering and fraud, and in connection with shareholder disputes. Much of his work involves multiple jurisdictions and cross-border issues of investigation and competing laws.

From 2012 to 2016, Mr Alford headed the Fraud Division at the Serious Fraud Office (SFO), where he was responsible for many of the UK's landmark white-collar cases. His work focused on investigations in banking and money markets, including the wide-ranging cases involving the manipulation of LIBOR, foreign-exchange benchmarks and the Bank of England's liquidity auctions.

© Law Business Research 2021

Mr Alford has extensive experience engaging with law enforcement and regulators around the world, including, in particular, the UK Financial Conduct Authority and the US Department of Justice. Mr Alford has significant experience managing parallel criminal and civil litigation, and has overseen significant data analysis projects and the advances in technology-assisted review and disclosure.

Before joining the SFO, Mr Alford spent 20 years in private practice as a barrister in London working in national and international criminal law. He was appointed Queen's Counsel in 2014.

Anupreet Amole
Brown Rudnick LLP

Anupreet Amole is a partner in Brown Rudnick's white-collar crime and regulatory investigations group. Anupreet has handled sensitive investigations in a wide range of multi-jurisdictional business crime matters, many involving allegations of bribery and corruption, fraud, misuse of confidential information, tax evasion and money laundering. Anupreet is listed by both *The Legal 500 UK* and *Who's Who Legal*.

Ryan J Andreoli
Jones Day

Ryan Andreoli is a partner at Jones Day in New York City, where he regularly represents financial institutions and other large corporations in securities class actions, shareholder derivative matters and complex commercial disputes. Ryan graduated from the New York University School of Law in 2003.

Jodi Avergun
Cadwalader, Wickersham & Taft LLP

Jodi Avergun is the chair of Cadwalader, Wickersham & Taft LLP's white-collar defence and investigations group, based in the firm's Washington, DC, office. Her practice focuses on representing corporations and individuals in criminal and regulatory matters involving, among other things, the Foreign Corrupt Practices Act (FCPA). Her experience in FCPA matters includes directing due diligence reviews in connection with mergers and acquisitions in a number of industries and jurisdictions; designing and implementing robust FCPA compliance policies, systems and training for corporate clients; and counselling clients in voluntary disclosures of FCPA violations. Jodi also advises clients in securities enforcement, healthcare and other white-collar matters, and has successfully represented both companies and senior executives in internal investigations, matters before regulatory bodies, including the Securities and Exchange Commission, and civil and criminal matters in federal court.

Jodi was an Assistant US Attorney and a member of the Senior Executive Service in the US Department of Justice for 17 years. She was recognised in the 2014 edition of *The Legal 500 US* as a 'Key Individual' in the white-collar criminal defence area and was named one of the 2016 '150 Women in White Collar' by *Corporate Crime Reporter*.

© Law Business Research 2021

Additionally, Cadwalader was named a 'Highly Recommended' firm for FCPA by *Global Investigations Review* in its 2016 rankings of the FCPA Bar in Washington, DC.

Amanda L Azarian
Jenner & Block LLP

Amanda Azarian is an associate at Jenner & Block's London office focusing on investigations, compliance and defence. Ms Azarian has extensive experience in working on a range of government enforcement actions in the United States and United Kingdom, including large, complex matters involving the SFO, NCA, DOJ, SEC and OFAC, with a concentration on economic crime. Her practice includes the representation of both corporates and individuals, conducting and advising on global internal investigations, defending against allegations relating to financial crime and responding to government requests, offering compliance advice including in relation to anti-bribery and corruption, anti-money laundering, and sanctions and developing and implementing tailored compliance programmes, due diligence and risk assessments. Prior to joining Jenner & Block, Ms Azarian worked for the Washington, DC and London offices of an international law firm. Ms Azarian received her law degree from the Catholic University of America, Columbus School of Law, where she served as a staff member of the Catholic University Law Review and interned for the Hon Heidi Pasichow at the Superior Court for the District of Columbia. She is admitted to practise in both Maryland and Washington, DC.

Robin Barclay QC
Fountain Court Chambers

Robin Barclay QC is a member of Fountain Court Chambers, London.

He is currently and has been repeatedly recognised by all the directories and his peers as a leading practitioner in international commercial civil and criminal fraud, bribery, money laundering, sanctions, market abuse and insider trading and a wide range of banking, financial services and regulatory and disciplinary investigations.

He was called to the Bar in 1999 and became a Queen's Counsel in 2020.

His practice comprises mainly high-profile complex litigation and is heavily weighted towards points at which commercial conduct straddles the line between civil, regulatory and criminal law – and in particular cross-border work involving banking and the financial markets. As well as trials and investigations, Robin's practice covers a range of interim applications and other matters, including civil and criminal search orders, freezing injunctions and restraint orders, directors' duties and liabilities, shareholder and derivative actions, disclosure orders and document production notices, internal investigations, company announcements, corporate self-reports and deferred prosecution agreements, unexplained wealth orders, immunity agreements, extradition, legal privilege, privacy and confidentiality, sanctions and criminal confiscation.

Robin is co-author of the leading book on the UK Bribery Act 2010 published by LexisNexis.

© Law Business Research 2021

Anthony S Barkow
Jenner & Block LLP

Anthony Barkow is co-chair of Jenner & Block's investigations, compliance and defence practice, and a member of the firm's markets and trading and government controversies practices. He represents companies and executives in global and national criminal and regulatory investigations. He also conducts internal investigations for corporations and other institutions, provides counsel to senior management on enforcement and compliance issues, and serves as a corporate monitor. As a federal prosecutor for 12 years in the United States Attorney's Offices for the Southern District of New York and the District of Columbia, and in Main Justice, he prosecuted some of the most significant international terrorism and white-collar criminal cases in the country. He has tried over 40 cases and briefed and argued more than 10 cases on appeal. During his government service, Mr Barkow was awarded the Attorney General's Award for Exceptional Service, the highest award bestowed by the Attorney General in the Department of Justice. He graduated from Harvard Law School, where he was Notes Office co-chair and supervising editor of the *Harvard Law Review*, and the University of Michigan.

Lisa H Bebchick
Ropes & Gray LLP

Lisa Bebchick is a partner in Ropes & Gray's litigation and enforcement practice group, based in New York. Lisa's practice focuses on complex commercial and real estate litigation and white-collar criminal defence and regulatory matters, including securities enforcement and internal investigations. She has represented individuals and institutions in connection with myriad high-stakes issues, including multimillion-dollar criminal and civil forfeiture proceedings and related matters. She has also represented clients in connection with investigations by SEC, FINRA, the US Attorney's Office and the Office of the New York Attorney General, and has represented clients who have been victims of investment frauds in attempting to recover losses and in defending against clawback actions brought by bankruptcy trustees.

Lisa regularly advises corporate clients in connection with pre-litigation contractual disputes, due diligence and whistleblower claims, and has extensive experience in handling bulge bracket bank regulatory work. Lisa has substantial experience in state and federal courts at the trial and appellate levels, as well as in mediation and arbitration.

Lisa is co-chair of Ropes & Gray's Women's Forum and a hiring partner for the New York office.

Benjamin A Berringer
Clifford Chance US LLP

Benjamin Berringer is an associate at Clifford Chance US LLP, where he focuses on cross-border investigations and complex commercial litigation. Ben represents both corporations and individuals in connection with regulatory investigations before the Commodity Futures Trading Commission, the Department of Justice and the Securities and Exchange Commission. Ben also advises on matters arising under cybersecurity,

© Law Business Research 2021

privacy and data protection laws. Ben received his BA from Williams College, his MSc in economics from SOAS and his JD from New York University School of Law.

Todd Blanche
Cadwalader, Wickersham & Taft LLP

Todd Blanche is a partner in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. He served for nearly a decade as an Assistant US Attorney for the Southern District of New York. As co-chief of the White Plains Division, he supervised investigations and prosecutions involving public corruption, securities fraud, bank and wire frauds, Medicare and federal programme frauds, RICO violations, violent crimes and other criminal violations. He also served as co-chief of the Violent Crimes Unit. Todd has extensive trial experience, serving as counsel in 15 federal jury trials. Todd is a recipient of the Director's Award from the US Department of Justice for Superior Performance as an Assistant US Attorney.

Todd received his undergraduate degree in political science and interdisciplinary studies from American University, and his law degree, *cum laude*, from Brooklyn Law School, where he was an editor of the *Brooklyn Law Review*. He held clerkships with the Hon Joseph F Bianco for the US District Court for the Eastern District of New York and the Hon Denny Chin of the US District Court for the Southern District of New York (both now judges of the US Court of Appeals for the Second Circuit).

William Boddy
McGuireWoods

William Boddy is a partner in McGuireWoods' London office. He is a risk-management and litigation strategist for global corporations and financial institutions. He represents clients in international arbitrations, before UK courts in complex multi-jurisdictional cases and in high-stakes regulatory proceedings. William's cases often involve allegations of fraud and applications for urgent injunctive relief, including freezing orders. His experience covers a range of industries, including technology, telecommunications, banking and oil and gas, in respect of which he has acted for both corporate and private clients.

Alongside his litigation practice, William advises on a variety of general commercial and compliance matters, including professional negligence, data privacy and security, contractual obligations and directors' duties, often in the context of insolvency. He also advises as to compliance with domestic and European Union regulations, including the GDPR, and anti-corruption laws such as the UK Bribery Act 2010.

Nicolas Bourtin
Sullivan & Cromwell LLP

Nicolas Bourtin is a litigation partner at Sullivan & Cromwell LLP, co-head of the firm's FCPA and anti-corruption group, and managing partner of the firm's criminal defence and investigations group. His practice focuses on white-collar criminal defence and internal investigations, regulatory enforcement matters, and securities and complex civil litigation.

© Law Business Research 2021

Mr Bourtin has represented individuals, corporations and financial institutions in numerous high-profile matters involving accounting fraud, antitrust, FIRREA, the FCPA, insider trading, money laundering, mortgage orientation and servicing, OFAC sanctions, securities fraud, tax fraud and trading. He has extensive experience in representing financial institutions in parallel regulatory and criminal investigations and representing non-US companies and individuals in connection with US investigations.

Mr Bourtin has conducted numerous jury trials and has argued frequently before the US Court of Appeals for the Second Circuit. He is frequently recognised as a leading practitioner in the area of white-collar criminal defence. Mr Bourtin also serves, *pro bono*, on the Criminal Justice Act panel for the Eastern District of New York, representing indigent defendants in federal criminal proceedings.

Mr Bourtin served for four years as an Assistant US Attorney in the Eastern District of New York, where he was involved in investigations, prosecutions and trials involving fraud, corruption, money laundering and other white-collar offences.

Michael Bowes QC
Outer Temple Chambers

Michael Bowes QC specialises in business crime, corruption, civil fraud, financial services and economic sanctions. He acts for corporate clients and senior managers in global investigations and for the SFO, FCA, CMA and Lloyd's of London. He advises companies in respect of US and EU sanctions. He acts for overseas regulators and is instructed in overseas cases as an expert in English law. He is regarded as an expert in civil and criminal crossover work and is described as 'one of the few specialist criminal practitioners in this area' (*The Legal 500* 2015) and as '[v]ery clever and has wide expertise, so is comfortable with criminal and civil work' (Financial Crime: Corporates, *Chambers* 2017). He is listed as a leading silk in the fields of financial services, financial crime (corporates) and financial crime (London) in *Chambers 2022*, and for banking and finance, business and regulatory crime, and fraud in *The Legal 500*. He is listed in *Who's Who Legal* 2021 as an expert in business crime defence. He sits as a Deputy High Court Judge (Queen's Bench Division) and as a Recorder of the Crown Court. He is a Bencher of the Honourable Society of the Middle Temple. He is a trustee of Transparency International UK and a co-chair of the UK Chapter of the International Section of the New York State Bar Association.

Ben Brandon
Mishcon de Reya LLP

Ben Brandon is a partner in the white-collar team at Mishcon de Reya LLP. He has recently returned to private practice after 15 years at a leading set of barristers' chambers in London, where he specialised in extradition, fraud and public law. He has appeared as an advocate in many of the most important extradition cases in recent years, from Abu Hamza to Julian Assange, acting for requesting states and requested persons. In that time, he appeared as advocate in extradition cases before Westminster Magistrates' Court, the High Court and the Supreme Court. Ben also acts for individuals who are the subject of abusive Interpol red notices, and in cases involving the unlawful disclosure of

© Law Business Research 2021

secret or confidential information. Ben formerly taught International Criminal Law at the London School of Economics and is a past chair of the business crime committee of the International Bar Association.

Matthew Bruce
Freshfields Bruckhaus Deringer

Matthew Bruce is co-head of Freshfields' global investigations and corporate crime practice in London and an experienced commercial litigator. Previously highlighted as one of the world's 40 leading investigations specialists under the age of 40 by *Global Investigations Review* and recommended by directories (including being listed as a leading investigations and business crime lawyer in *Chambers*, *Who's Who Legal* and *The Legal 500*), Matthew has led a number of major corporate internal and external investigations for blue-chip clients in all sectors arising from allegations of bribery and corruption, fraud, misaccounting and human rights abuses. Recent matters have engaged Asia, the Middle East, former CIS territories and Africa. Matthew has been a partner since 2012.

John D Buretta
Cravath, Swaine & Moore LLP

John D Buretta is a partner in Cravath's litigation department and a former senior official at the US Department of Justice (DOJ). He has represented global companies, boards of directors, audit committees, senior management and general counsels of public and private companies, law firms, and former US and foreign government officials with respect to internal investigations, criminal defence, regulatory compliance and related civil litigation matters. He has handled matters involving the US Foreign Corrupt Practices Act (FCPA), antitrust laws, securities fraud and disclosure regulations, money laundering and anti-money laundering controls, trade sanctions, export controls, cyber intrusion and tax compliance, and has appeared for clients before numerous US enforcement agencies. Mr Buretta served for 11 years in the DOJ, including supervising the Criminal Division, where he oversaw nearly 600 prosecutors in international investigative matters involving corporate fraud, the FCPA, insider trading, healthcare fraud, money laundering, the Bank Secrecy Act, trade sanctions, asset forfeiture, cybercrime, intellectual property theft and public corruption. He currently serves as an independent monitor in separate appointments by the DOJ and the US Department of Transportation.

Daniel Burget
BDO USA, LLP

Daniel Burget is a director in the forensics practice at BDO USA providing anti-money laundering compliance and fraud investigation services. He specialises in leading model validations and technical testing of anti-money laundering and economic sanctions compliance systems. Daniel has extensive financial fraud investigative experience gained over a 26-year career as a special agent with the criminal investigation division of the Internal Revenue Service (IRS-CI), specialising in digital forensics relating to

© Law Business Research 2021

cyber-enabled financial crimes. Daniel has conducted and led complex financial investigations involving tax fraud, money laundering, Bank Secrecy Act violations, terrorism financing and related financial crimes. He has particular expertise in digital forensics in financial crimes from leading IRS-CI's Electronic Crimes Program.

Matthew Burn
Ropes & Gray LLP

Matthew Burn is a member of Ropes & Gray's litigation and enforcement practice group, based in London. Matthew's practice focuses on corporate and financial crime defence, contentious regulatory matters and internal investigations. Matthew has extensive experience in advising both corporations and individuals facing complex cross-border investigations and prosecutions relating to allegations of bribery and corruption, money laundering, fraud and other types of misconduct or regulatory failings.

Matthew was previously seconded to a global financial institution and a leading professional services firm to assist with internal and regulatory investigations.

Matthew joined Ropes & Gray in 2018 from a magic circle firm in London.

James Carlton
Fox Williams LLP

James Carlton is a partner at Fox Williams LLP specialising in all areas of business crime and regulation. Sources say he 'inspires total confidence from his clients, has a wonderful knack of making them feel comfortable and superbly represented, while not pulling any punches in terms of problems they may face' (*Chambers* 2017).

James has been instructed in a number of the largest and most complex white-collar investigations and prosecutions brought by the UK regulatory and prosecuting authorities, including the Serious Fraud Office and the Financial Conduct Authority, relating to, among other things, allegations of fraud, money laundering, insider dealing, market abuse, and bribery and corruption. Increasingly these have significant international dimensions and considerations.

James also has great expertise in the conduct of public inquiries. He has been instructed by interested parties in a large number of the highest-profile public inquiries, including, among others, the BSE, *The Marchioness*, Leveson, Pollard and Victoria Climbié inquiries.

He has been instructed on a number of complex and cross-border regulatory investigations for senior executives. He has also been instructed in relation to the regulatory investigations into the manipulation of LIBOR, EURIBOR and FX. He has extensive experience of high-profile corporate investigations involving complex issues of financial crime, bribery and corruption, employee fraud and significant acts of dishonesty.

© Law Business Research 2021

Sinead Casey
Linklaters LLP

Sinead Casey is a partner in Linklaters' employment and incentives group in London. She advises on a broad range of employment advisory and regulatory issues, including executive appointments and terminations, internal and regulatory investigations, group reorganisations and restructurings, outsourcings and the employment aspects of public and private M&A deals. She has particular expertise working with clients on crisis management mandates, advising them on their most challenging and sensitive HR-related issues as they navigate their way through a crisis.

Sinead's typical advisory work includes counselling on recruitment and termination, redundancy exercises, employment contracts, policies and procedures, grievance and disciplinary proceedings, the implementation of pension and other benefit changes, trade disputes and corporate governance-related issues.

Sinead represents clients before employment tribunals, the High Court and the Court of Appeal, including in unfair dismissal, discrimination and breach of contract claims.

Francesca Cassidy-Taylor
Brown Rudnick LLP

Francesca Cassidy-Taylor is a chartered legal executive and a member of Brown Rudnick's white-collar crime group. Her practice focuses on corporate and financial crime, principally cases involving international bribery and corruption, commercial fraud and money laundering. Francesca advises both individual and corporate clients and has been involved in a number of high-profile domestic and international investigations conducted by enforcement agencies, including the SFO, the US DOJ, HMRC, the CMA and the NCA. She is experienced in dealing with matters involving foreign and cross-border investigations, including requests for mutual legal assistance and extradition.

Jessica Chappatte
Herbert Smith Freehills LLP

Jessica Chappatte is a senior associate in Herbert Smith Freehills LLP's corporate crime and investigations team in London. Jessica advises both corporate and individual clients in all aspects of business crime, with a particular emphasis on investigations relating to bribery, corruption, fraud and money laundering. Jessica has worked closely with the UK SFO, FCA and HMRC on various matters.

Jessica's more recent experience includes successfully defending one of the Barclays executives charged with allegations of fraud arising from conduct during the Barclays capital raisings of 2008, advising a financial institution regarding an FCA criminal investigation and prosecution against a former employee for insider trading, and advising a FTSE 250 company in an SFO investigation arising from the actions of third parties in Asia.

© Law Business Research 2021

Eric Christofferson
DLA Piper LLP

Eric Christofferson is an experienced litigation and compliance lawyer in DLA Piper's Boston office and is a member of the firm's white-collar group. He represents corporations and individuals in government investigations, internal investigations, criminal and regulatory proceedings, and civil litigation. Prior to joining DLA Piper, Eric served as an Assistant US Attorney in the District of Massachusetts, primarily prosecuting economic and other white-collar crime. Eric, whose practice focuses on the life sciences and financial services sectors, is an experienced courtroom lawyer who has tried more than 15 criminal and civil jury trials during his career.

Bradley A Cohen
Mayer Brown

Bradley Cohen is an associate in Mayer Brown's New York office and a member of the litigation and dispute resolution practice. His practice focuses on advising corporate entities, including domestic and non-US financial institutions, on compliance and enforcement matters, regulatory investigations, and banking and financial services-related litigation.

In particular, Brad counsels clients on issues related to anti-money laundering obligations under the Bank Secrecy Act, anti-bribery and corruption requirements under the Foreign Corrupt Practices Act, and economic and trade sanctions administered by the Office of Foreign Assets Control. He also advises financial institutions on various registration, reporting and business conduct requirements arising under the Dodd-Frank Act and other US laws and regulations. From a cross-border perspective, Brad provides US financial institutions with guidance on the impact of recent EU legislative efforts, including the recast Markets in Financial Instruments Directive and the European Market Infrastructure Regulation.

Jonathan Cotton
Slaughter and May

Jonathan Cotton is a partner in Slaughter and May's disputes and investigations group. He covers a range of cases involving contractual disputes, competition disputes and restructuring and insolvency matters. He also often advises on contentious aspects of corporate transactions, including takeovers.

He is particularly experienced in matters involving allegations of wrongdoing in its various forms. On the civil side, these have included cases involving the 'theft' of confidential information by employees and competitors, conspiracy and civil fraud. On the criminal and regulatory side, he has been involved in investigations and criminal prosecutions, cases concerning cartels, and regulatory cases concerning the UK Bribery Act, the Proceeds of Crime Act, the Fraud Act, Financial Services and Markets Act 2000, export controls and sanctions, and Companies Act offences.

The major investigations and disputes on which he has been engaged span business sectors including telecoms, investment banking, investment management, technology, heavy manufacturing, natural resources and fast-moving consumer goods.

© Law Business Research 2021

Gail E Crawford
Latham & Watkins

Gail Crawford, global chair of Latham's data and technology transactions practice, helps clients navigate complex data privacy and security matters, as well as to license, develop and exploit disruptive technology.

Ms Crawford advises many of the world's leading global technology companies on multifaceted and precedent-defining data privacy and security matters. Her work in the data privacy and security space encompasses advising on compliance programmes, product counselling, responding to data breaches and regulatory inquiries, advising on optimal organisational structures, and supporting large, strategic alliances and M&A transactions. She also helps clients navigate a myriad of issues in technology law, including commercial contracts, collaborations, and intellectual property.

Ms Crawford draws on her experience handling some of the most complicated and sensitive data privacy matters in the global market to provide pragmatic and commercially driven counsel. She brings a deep understanding of the innate value of data and the complex, ever-changing global regulatory framework to help clients achieve their business objectives.

Ms Crawford regularly writes and speaks on topics related to data privacy and disruptive technology, and serves as an editor of the Latham & Watkins Global Privacy & Security Compliance Law Blog.

Nikki Cronin
Willkie Farr & Gallagher LLP

Nikki Cronin is an associate in the global trade and investment practice group in Washington, DC. Nikki advises clients on government regulations relating to international trade and investment, with a particular focus on US economic sanctions. Nikki regularly advises both domestic and foreign clients on compliance and enforcement matters relating to US economic sanctions and export controls for a variety of industries, including financial institutions, private equity firms, oil and gas and media companies.

Mellissa Curzon-Berners
Mishcon de Reya LLP

Mellissa Curzon-Berners is an associate in the white-collar crime and investigations group at Mishcon de Reya with a broad range of experience acting for both corporate and individual clients facing investigations into fraud, bribery, money laundering and other regulatory matters. She advises individuals subject to Interpol red notices and mutual legal assistance requests and has cross-jurisdictional investigation experience involving regulatory and prosecuting authorities. Mellissa has a particular expertise in money laundering and is frequently instructed to advise corporate and individual clients on their obligations under the UK anti-money laundering regime. She also assists corporate clients to design and implement effective compliance policies.

© Law Business Research 2021

Eleanor Davison
Fountain Court Chambers

Eleanor Davison is a barrister at Fountain Court Chambers specialising in cross-border white-collar crime, fraud, corruption and contentious regulatory cases. Consistently recognised as expert in the fields of financial crime, financial crime (corporates), financial services and money laundering by *The Legal 500* and *Chambers and Partners*, she has recently been described as having 'a phenomenal brain and in-depth knowledge of her area of expertise. She is quick-witted, alert to opposing arguments and a delight to work with – a real star to watch' (*Chambers and Partners UK* 2019, Financial Crime). The directories also describe her as '[v]ery good and particularly experienced in complex investigations involving financial institutions'. Eleanor was listed in *Who's Who Legal* as a Future Leader in investigations in 2018.

Caroline Day
Kingsley Napley LLP

Caroline Day is a partner at Kingsley Napley LLP. She is an investigations specialist and frequently represents corporates and individuals in serious, high-profile and complex investigations. She has extensive experience in leading internal investigations and reviews on behalf of companies and organisations concerning a wide range of allegations of misconduct and financial crime, including fraud, corruption and money laundering, often involving multiple jurisdictions. Caroline has a particular interest in cross-border cases and advising on the complex issues that arise in global investigations. She advises companies and individuals involving investigations and prosecutions by various agencies, including the Serious Fraud Office, the Financial Conduct Authority and the Competition and Markets Authority.

Caroline sits on the executive committee of the Fraud Lawyers Association. She was recognised in Global Investigations Review's 100 'Women in Investigations 2018' and listed by *Who's Who Legal* in *Investigations Future Leaders – Partners* 2021 and as a Global Leader in *Business Crime Defence* 2021.

Tapan Debnath
ABB

Tapan Debnath is head of integrity, regulatory affairs and data privacy – process automation, at ABB. He was previously senior legal counsel for Nokia, handling ethics and compliance investigations in Europe, the Middle East and Africa, and had served as the compliance lead for the Nokia Enterprise Business Group and acted as lead trade compliance counsel. Prior to joining Nokia, Tapan was a prosecutor at the UK's Serious Fraud Office, where he investigated and prosecuted major international economic crime cases. Tapan is an experienced English-qualified solicitor specialising in corporate crime and compliance. He also holds a certificate in financial crime from the University of London.

© Law Business Research 2021

Michelle de Kluyver
Addleshaw Goddard LLP

Michelle de Kluyver is a partner in Addleshaw Goddard's global investigations and contentious regulatory group. Michelle has extensive experience in complex, cross-border financial crime investigations including bribery and corruption, financial sanctions, money laundering and fraud, and also advises clients on related directors' duties and compliance issues. Michelle is named as a Thought Leader in *Who's Who Legal: Business Crime Defence* and a Leading Individual in *Who's Who Legal: Investigations* and *Who's Who Legal: Trade & Customs (International Sanctions)*. Michelle was selected by *Global Investigations Review* in 2015 as one of 100 remarkable women investigation specialists operating across the world. *Who's Who Legal* says: 'Michelle receives widespread plaudits from international peers for her "fantastic" work on cross-border international investigations relating to fraud, bribery and corruption claims.' Michelle and co-author Ben Koehne contributed the chapter on Directors' Duties for the sixth edition of Sweet & Maxwell's *A Practitioner's Guide to Directors' Duties and Responsibilities*.

William H Devaney
Baker McKenzie LLP

William (Widge) Devaney is a partner in Baker McKenzie's North America litigation group in New York, co-chair of the firm's global compliance and investigations group and co-chair of the North American government enforcement practice. He was an Assistant United States Attorney in the District of New Jersey, where he was a member of the Securities Fraud Unit. Widge's main areas of practice are white-collar criminal defence, investigations, compliance and complex civil litigation.

Widge is the author of multiple publications involving such topics as the FCPA, investigations and corporate compliance programmes. He often appears in the print media commenting on current criminal matters.

Widge received an AB and JD from Georgetown University, and an LLM from Cambridge University. He clerked for the Hon Oliver Gasch on the US District Court for the District of Columbia. He is a member of the New York Bar.

Mehboob Dossa
McGuireWoods

Mehboob (Mebs) Dossa is a partner in McGuireWoods' London office. He specialises in advising multinationals on compliance with EU and UK data privacy and security laws, in particular compliance with GDPR and e-privacy regulations, cross-border data transfers, security incident management, handling of data subject access requests, processor arrangements, and addressing data privacy and security issues in supply chain and M&A transactions. Mebs holds the CIPP/E certification as a Certified Information Privacy Professional from the International Association of Privacy Professionals.

Mebs also specialises in advising multinationals, capital providers, independent sponsors, family offices, private equity portfolio companies and executives on a variety of matters, including mergers and acquisitions, co-investments, leveraged buyouts, joint

© Law Business Research 2021

ventures, restructuring, setting up operations in the United Kingdom, structured equity investments, divestitures, commercial/supply chain transactions and corporate governance matters. He also advises emerging-growth and early-stage companies. Mebs' practice over the years has focused on UK-inbound work from various jurisdictions, in particular the United States and Canada, and has involved a diverse scope of industries including healthcare, private equity, energy, pharmaceuticals, consumer goods and services, technology and financial services.

J Robert Duncan
Cadwalader, Wickersham & Taft LLP

Robert Duncan, an associate in Cadwalader's white-collar defence and investigations group, advises clients in a variety of criminal, civil and regulatory matters, including compliance with the Foreign Corrupt Practices Act, and accounting and reporting regulations.

Prior to law school, Robert was a senior audit, assurance and risk advisory associate at a Big Four accounting firm. He is a licensed certified public accountant in the Commonwealth of Kentucky. Robert has taught undergraduate courses in accounting and auditing at the McIntire School of Commerce at the University of Virginia, where he has been a visiting lecturer and instructor.

Robert received his JD from the University of Virginia, where he served as a senior editor for the Virginia Law and Business Review. He earned his MS in accounting from the McIntire School of Commerce at the University of Virginia and his BS in accounting from Ball State University's Honors College. Robert is admitted to practise in the State of New York and the District of Columbia.

Ahmad El-Gamal
Willkie Farr & Gallagher LLP

Ahmad El-Gamal is an associate in Willkie's global trade and investment group in Washington, DC. Ahmad provides advice to both domestic and foreign clients on government regulation of international trade and investment, particularly with regard to the Committee on Foreign Investment in the United States, economic sanctions and export controls.

Tom Epps
Cooley LLP

Tom Epps is the head of Cooley's London white-collar defence and investigations team. Tom is recognised in the United Kingdom and internationally as a leading white-collar crime lawyer. He has been involved in many of the United Kingdom's largest and most complex investigations in the past 20 years.

Tom has substantial experience representing those facing investigations brought by all the major UK enforcement agencies, particularly investigations with an international aspect. He is advising clients in the majority of the Serious Fraud Office's most high-profile investigations, nearly all of which involve substantial international dimensions. He

© Law Business Research 2021

frequently advises companies and senior individuals facing sensitive investigations and regulatory issues and is often called on to assist suspects, whistleblowers and witnesses. Tom is regularly recognised as a thought leader and highly ranked in the leading legal directories for white-collar crime. He is recognised by *Who's Who Legal* 2021 as a Global Elite Thought Leader for Business Crime and as a Global Leader for Investigations and Asset Recovery. *Chambers and Partners UK* ranks Tom in the top bands for his representation of individuals and corporates, as well as for high net worth individuals in financial crime investigations. He is recognised as a leading individual for Fraud: White Collar Crime by *The Legal 500*.

Jaime Orloff Feeney
Ropes & Gray LLP

Jaime Orloff Feeney, a counsel at Ropes & Gray in Chicago, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Aleesha Fowler
Baker McKenzie LLP

Aleesha Fowler is a senior associate in Baker McKenzie's North America litigation and government enforcement practice group in Washington, DC. Aleesha focuses her practice on white-collar criminal defence, corporate compliance and complex civil litigation that often arises from parallel regulatory investigations. She advises individuals and multinational companies on issues relating to anti-corruption and fraud, and routinely assists companies in implementing compliance programmes that align with regulatory standards. Aleesha also has extensive experience with advising multinational companies on supply chain compliance and ESG-related risks, and she is an editor of Baker McKenzie's Global Supply Chain Compliance Blog.

Aleesha received her BA from the University of Virginia (with Distinction), and her JD from Cornell University, where she was an Honor's Fellow and President of Cornell's Black Law Students Association.

Sona Ganatra
Fox Williams LLP

Sona Ganatra is a partner at Fox Williams LLP specialising in financial services regulatory investigations and internal investigations. She has extensive experience in advising firms and individuals on a broad range of regulatory issues, including conduct rule breaches; allegations of financial crime (such as money laundering, bribery and corruption, and fraud), as well as issues arising in the fintech sector relating to consumer-credit activities, payment services and e-money. She is regularly instructed in relation to FCA and SFO investigations, prosecutions and enforcement action against corporates and senior individuals. She also has extensive experience of high-profile corporate investigations advising

© Law Business Research 2021

on issues of self-reporting to and liaising with a variety of regulatory bodies and prosecuting authorities.

Sona is ranked as a Leading Individual by *The Legal 500*. Sources describe her as 'energetic and detailed; incredibly personable and reassuring' and having an 'incredible knowledge of the area' (*The Legal 500*). She is recognised for understanding 'the commercial realities and personal pressures of investigations and proceedings and help[ing] clients manage both' (*The Legal 500*) and making 'a concerted effort to engage the board and non-board personnel to gauge the severity of the issue. She is very detailed and diligent' (*Chambers Client Feedback*).

Earlier in her career, Sona was seconded to the Enforcement Division of the Financial Services Authority, where she appeared before the Regulatory Decisions Committee and participated in settlement discussions with financial institutions. This provided her with invaluable insight into regulatory investigations and disciplinary actions.

Jacob Gardener
Walden Macht & Haran LLP

Jacob Gardener is an experienced litigator who represents corporations and individuals in criminal, civil and regulatory matters. Jake has extensive experience managing internal and government investigations, complex commercial disputes, and appeals. He has helped lead internal investigations into high-stakes matters involving alleged violations of the FCPA and securities laws. Jake has also successfully handled numerous civil cases in a variety of areas, including commercial contract disputes, mortgage-backed securities litigation, shareholder derivative actions, bankruptcy and employment law. He has significant courtroom experience, including briefing and arguing several appeals and dispositive motions in criminal and civil cases. Before joining Walden Macht & Haran, Jake clerked for the Hon Dennis Jacobs of the US Court of Appeals for the Second Circuit and the Hon Naomi Reice Buchwald of the US District Court for the Southern District of New York. In addition, Jake served for several years as a New York City firefighter. His academic scholarship has been published in the *Journal of Criminal Law and Criminology* and the *Boston University Journal of Science and Technology Law*. Jake is a graduate of Yale Law School and Stanford University.

Meredith George
Clifford Chance US LLP

Meredith George is an associate in the litigation and dispute resolution practice of Clifford Chance, specialising in government enforcement and litigation focusing on investigations, including investigations involving issues of antitrust violations and market manipulation. Her relevant experience includes defending a major financial institution in class action litigation alleging a conspiracy to manipulate platinum and palladium benchmarks and related derivatives prices, and representing a multinational oil and gas company in a US CFTC investigation into certain transactions in the European physical market with downstream effects in the US futures market. She is a graduate of Rice University and Duke University School of Law and is admitted to practise in New York.

© Law Business Research 2021

Meghan Gilligan Palermo
Ropes & Gray LLP

Meghan Gilligan Palermo is an associate at Ropes & Gray in New York, who frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Charlotte Glaser
Cadwalader, Wickersham & Taft LLP

Charlotte Glaser is an associate in Cadwalader's white-collar defence and investigations group, resident in the London office. Charlotte has advised clients involved in multi-jurisdictional bribery and corruption, complex fraud and money laundering investigations commenced by a number of enforcement agencies, including the Serious Fraud Office and HM Revenue and Customs. She has experience in representing individuals in relation to contentious regulatory matters, in particular, investigations conducted by the Financial Conduct Authority, the Competition and Markets Authority and the Brazilian competition regulator, the Administrative Council for Economic Defence. Charlotte also has experience advising multinational corporations in relation to internal investigations. Her advisory work incorporates anti-money laundering compliance, international sanctions regimes, and bribery-related and corruption-related matters. Charlotte previously practised as a barrister specialising in criminal law.

Emily Goddard
Clifford Chance LLP

Emily Goddard is an associate in Clifford Chance's litigation and dispute resolution group in London. She advises on a range of contentious matters, and has particular experience in investigations and regulatory enforcement action, white-collar crime and business and human rights (BHR).

Her BHR work includes: advising global clients on human rights and environmental, social and governance (ESG) issues, including due diligence and responsible investment frameworks (she has a particular interest in hardening regulation related to human rights and environmental due diligence, and the potential for increased litigation in future); advising clients on the UK Modern Slavery Act 2015 and other similar standards, including appropriate implementation of anti-human trafficking and slavery measures within their organisations, reporting requirements and supply chain due diligence; and advising on policy content and implementation consistent with the UN Guiding Principles on Business and Human Rights and on related corporate governance.

Emily leads the firm's ESG investigations working group, which focuses on the firm's BHR and investigations practice, including investigations into clients' supply chain or security incidents.

© Law Business Research 2021

Chloe Gordils
Ropes & Gray LLP

Chloe Gordils is an associate at Ropes & Gray's New York office and is a member of the firm's litigation department.

Duncan Grieve
Cadwalader, Wickersham & Taft LLP

Duncan Grieve is an associate in Cadwalader's white-collar defence and investigations group, resident in the London office. Duncan advises a range of organisations, including multinationals, both on internal corporate investigations and during investigation or prosecution by regulatory bodies including the Serious Fraud Office, the Financial Conduct Authority, the US Department of Justice and the Securities and Exchange Commission. He has experience in dealing with international investigations involving issues in foreign jurisdictions, including Brazil, Russia, China, India, Romania, the Czech Republic, Mozambique, Canada and Japan. Duncan also represents individuals subject to internal, regulatory and criminal investigation. Duncan speaks fluent Portuguese and spent two years in Brazil working with a Brazilian law firm, where he advised corporate and individual clients in investigations stemming from the *Lava Jato* (*Operation Car Wash*) investigation.

Jaya Gupta
Addleshaw Goddard LLP

Jaya Gupta is a partner in Addleshaw Goddard's London corporate division where she leads the corporate governance team. She has over 25 years' experience providing support to clients on governance and compliance issues, as well as on a wide range of complex cross-border and UK corporate transactions. Jaya's transactional experience extends to public takeovers, private M&A and recapitalisations across a variety of sectors.

Kevin Harnisch
Norton Rose Fulbright LLP

Kevin Harnisch is the US head of regulation, investigations, securities and compliance at the firm. He is a litigator who defends clients before the United States Securities and Exchange Commission (SEC), FINRA and other self-regulatory organisations, the Department of Justice, the US Commodity Futures Trading Commission, US Attorneys' offices and federal courts. He handles matters relating to securities enforcement defence, internal investigations and anti-corruption issues, and represents corporations (and their directors and officers), broker-dealers, hedge funds, private equity funds and investment banks.

Kevin served as a branch chief in the Division of Enforcement of the SEC, where he led cases regarding financial fraud, market manipulation, insider trading, the Foreign Corrupt Practices Act and municipal bond offerings.

© Law Business Research 2021

Kevin has significant experience defending public companies in a wide array of government agency investigations. Those investigations often pertain to such issues as the accuracy of financial statements, undisclosed related-party transactions, the adequacy of internal controls, the FCPA and other anti-corruption laws, responses to whistleblowers, and potential insider trading.

He is also active in representing broker-dealers in various matters, including in anti-money laundering and suspicious activity reporting issues, market manipulation, order handling and best execution, managing conflicts of interest, the reasonableness of supervision, and the effectiveness of internal controls.

Rodger Heaton

McGuireWoods

An accomplished federal prosecutor and litigation partner, Rodger Heaton has deep experience handling high-stakes matters involving cybersecurity issues. During his tenure at the US Attorney's Office for the Central District of Illinois, Rodger supervised investigations and tried dozens of jury trials to verdict in cases involving fraud, public corruption, money laundering, price-fixing, tax evasion, false claims and computer crimes. He led the prosecution of significant procurement fraud cases and initiated multi-agency task forces on cybercrime and public corruption throughout Central Illinois. Rodger represents clients in internal and criminal investigations, trials and appeals. He advises foreign, multinational, and domestic corporate and individual clients in internal investigations regarding electronic evidence and computer intrusion matters.

David B Hennes

Ropes & Gray LLP

David Hennes, a partner resident in Ropes & Gray's New York office, serves as co-chair of both the firm's corporate and securities litigation practice and investment banking industry group. David has more than 25 years of experience in litigating a broad array of corporate disputes, with an emphasis on complex corporate litigation, securities cases, corporate-control disputes and enforcement litigation. He regularly represents buyers, sellers and financial advisers in all forms of litigation. He frequently handles complicated federal securities class actions and state law derivative actions, and advises boards and board committees (including special litigation committees) on their responses to these litigations. David has represented corporate and individual clients in all aspects of these matters at the trial and appellate levels in federal and state courts throughout the United States, as well as in non-public SEC, FINRA and state securities investigations.

David has been consistently recognised by *Chambers USA: America's Leading Lawyers for Business* as a leading individual in general commercial litigation. *The Legal 500* has named David as a leading lawyer for M&A defence litigation. *Chambers* describes David as 'an outstanding lawyer who has excellent judgment, is responsive 24/7 and gives excellent, thoughtful and practical business-oriented advice'. *The Legal 500* calls him a 'first-rate litigator' and 'solution-oriented'. David has also been recognised by *Benchmark: Litigation* as a New York Litigation Star.

© Law Business Research 2021

John M Hillebrecht
DLA Piper LLP

John M Hillebrecht is the US national co-chair of DLA Piper's white collar, corporate crime and investigations practice. Immediately prior to joining DLA Piper in 2010, John served for 15 years as an Assistant United States Attorney in the Southern District of New York (SDNY), garnering extensive trial, appellate and supervisory experience.

He has served as lead or sole counsel in more than 20 jury trials and approximately 50 Second Circuit appeals. John has represented entities and individuals in the crosshairs of some of the highest-profile criminal investigations of recent years, including the 'expert network' insider trading cases, RMBS fraud prosecutions, the SDNY investigation regarding possible corruption in Governor Cuomo's 'Buffalo Billion' and related development projects, numerous rate-fixing cases (including the LIBOR, FX and ISDAfix manipulation cases), the GM ignition switch case, the ongoing Fiat Chrysler emissions control 'defeat device' investigation, and various FCPA investigations (including the 'Sons and Daughters' DOJ and SEC investigation into banks' hiring practices in China and an ongoing investigation involving one of the world's largest petroleum companies) and False Claims Act matters. He also regularly represents pharmaceutical and medical device companies and individuals in various kinds of investigations.

John is recommended in *The Legal 500 United States* and recognised in *The Best Lawyers in America*. In December 2015, *The National Law Journal* recognised John as one of the top white-collar practitioners in the country.

Louise Hodges
Kingsley Napley LLP

Louise Hodges is the head of the criminal department at Kingsley Napley LLP. She specialises in all fraud and business crime litigation, including investigations and prosecutions by the Financial Conduct Authority, the Serious Fraud Office (SFO), the National Crime Agency, HM Revenue and Customs, the City of London Police and the Crown Prosecution Service.

She is a lead partner in the Kingsley Napley financial services group and internal investigations team. Louise has a particular interest in cross-border cases representing companies and individuals. Her cases frequently have an international dimension, including involving the US Department of Justice, Federal Bureau of Investigation, Securities and Exchange Commission and US Commodities Futures Trading Commission as well as European prosecutors and regulators, including Consob, BaFin and FINMA. She was part of the team representing Tesco in the deferred prosecution agreement with the SFO. Louise is a past chair of the Fraud Lawyers Association and former vice chair of the European Criminal Bar Association. She is listed as a Global Elite Thought Leader in *Who's Who Legal: Investigations* 2021 and as a Thought Leader in *Business Crime Defence* 2021 and *Thought Leaders: GIR – Investigations* 2021.

© Law Business Research 2021

Daniel Igra
Nokia Corporation

Daniel Igra is legal counsel for Nokia, handling ethics and compliance investigations in Europe and Latin America. Prior to joining Nokia in November 2019, Daniel was a prosecutor at the UK's Serious Fraud Office, where he investigated and prosecuted major international economic crime cases. Daniel is an experienced English-qualified solicitor specialising in corporate crime.

Mary Jordan
Baker McKenzie LLP

Mary Jordan is a senior associate in Baker McKenzie's London office. Mary advises clients in relation to corporate investigations, regulatory engagement and enforcement, business crime, compliance and risk, and commercial and criminal litigation. She has a particular focus on financial institution clients in the regulated sector, handling domestic and international investigations and their related disputes on behalf of firms and individuals.

Mary was an undergraduate at Oxford University (Wadham College) and undertook her postgraduate legal studies at the College of Law in London.

Marie Kavanagh
Cooley LLP

Marie Kavanagh advises companies and senior individuals facing criminal and regulatory investigations carried out by all the leading UK authorities including the Serious Fraud Office (SFO), the Financial Conduct Authority and others. She advises suspects and witnesses in cases involving allegations of complex fraud, bribery and corruption, money laundering and other types of misconduct, often with a cross-border element. Marie acts for clients in both internal investigations and those led by enforcement agencies.

Marie has advised clients in relation to high-profile SFO investigations, including its investigations into Glencore, Quindell plc, Euribor, Barclays/Qatar, Rolls-Royce plc, Tesco plc, ENRC Ltd, Serco, Sweett Group plc, Libor and FX.

Marie is recommended by *Who's Who Legal* as a Future Leader (Non-Partners) in its Investigations 2020 and 2021 editions. Its 2020 edition states: 'Marie Kavanagh is "head and shoulders above the rest". Clients are "always reassured by her advice and rigour" and dub her "an undoubted star of the future" who is "extremely hardworking and wonderfully diligent in all manner of tasks".' Marie is also listed in *Expert Guides* as a Rising Star for White Collar Crime 2021 and in *The Legal 500* as a Rising Star for Fraud: White Collar Crime (Advice to Individuals) 2022.

© Law Business Research 2021

Ali Kirby-Harris
Freshfields Bruckhaus Deringer

Ali Kirby-Harris is a partner based in the dispute resolution team of Freshfields' London office. Ali has significant experience of complex, large-scale contentious mandates. She has a wide-ranging practice based on managing both commercial litigation and global internal and criminal investigations. Ali specialises in cases involving bribery and corruption issues and has significant experience of disputes involving accounting fraud and contentious matters arising from audit mandates. Ali advises on the related area of compliance risk management, including compliance with business and human rights standards, modern slavery law compliance and anti-terrorist financing regimes. She principally advises corporate clients, as well as financial sponsors on pre-deal and post-deal disputes. Her experience includes advising on both domestic litigation and multinational disputes involving multiple jurisdictions.

Anna Kirkpatrick
Clifford Chance LLP

Anna Kirkpatrick is a senior associate in Clifford Chance's litigation and dispute resolution practice. Anna specialises in ESG, business and human rights, international law and international arbitration. Anna's experience also includes the design and implementation of human rights policies and processes, human rights impact assessments and due diligence. She advises international organisations, governments and corporates on ESG considerations and human rights and the implementation of the soft law standards, such as the UNGP, for a wide range of businesses. Anna also represents clients in addressing allegations of complicity; assessing the legal and non-legal issues arising out of human rights impacts; and advising on specific human rights related issues such as labour protections for workers, the provision of security in high-risk jurisdictions and modern slavery. She is a trustee of Lawyers against Poverty and the diversity and inclusion officer of the IBA Business and Human Rights Committee.

Celeste Koeleveld
Clifford Chance US LLP

Celeste Koeleveld has more than 25 years of experience in government enforcement, regulatory and civil litigation matters that span federal, state and local government in the United States. During her career, she has held senior positions in the US Attorney's Office for the Southern District of New York (SDNY), the New York State Department of Financial Services (DFS) and the New York City Law Department. Ms Koeleveld represents clients, both corporates and individuals, with regulatory compliance, internal investigations and all phases of civil, criminal and regulatory litigation, from inception through the appellate process. Her significant government experience imparts a particularly insightful perspective to her advice and counsel in enforcement and regulatory matters.

Prior to joining Clifford Chance, Ms Koeleveld served as General Counsel at DFS, where she handled a broad spectrum of regulatory and enforcement actions, including

© Law Business Research 2021

disciplinary and enforcement proceedings. In addition, Ms Koeleveld served for 17 years in SDNY, rising to Chief of the Criminal Division, where she led a team of more than 160 Assistant US Attorneys and oversaw all criminal investigations and prosecutions. Ms Koeleveld also served for eight years as Executive Assistant Corporation Counsel at the New York City Law Department, providing legal advice to city agencies responding to government investigations from a variety of federal, state and local prosecutors and investigative bodies.

Ellen Lake
Clifford Chance LLP

Ellen Lake is a senior associate in Clifford Chance's international investigations practice. Her practice covers investigations, crisis management, internal risk management and enforcement defence across multiple sectors, where she has more than a decade's experience of advising in particular on financial crime, white-collar crime, compliance failings, internal investigations, whistleblowing reports, contentious regulatory and tech matters. She advises on a broad range of actions brought by UK authorities, as well as on complex cross-border investigations in multiple jurisdictions, particularly criminal and regulatory investigations and enforcement actions. Ellen works with a broad range of corporate and financial services clients and has completed a number of client secondments, including to a major bank where she ran an in-house legal team responding to a section 166 skilled person investigation into financial crime failings.

Sarah Lambert-Porter
Ropes & Gray LLP

Sarah Lambert-Porter is a senior associate in Ropes & Gray's litigation and enforcement practice group, based in London.

Sarah's practice focuses primarily on financial crime including bribery and corruption, terrorist financing, money laundering, fraud and other misconduct and regulatory failings. She has substantial experience advising financial institutions in relation to internal investigations and complex cross-border contentious regulatory matters, and criminal investigations and prosecutions. Sarah also advises in relation to the United Kingdom's Senior Managers and Certification Regime.

Sarah was previously seconded to a global financial institution to assist with the design and implementation of controls in relation to the Senior Managers and Certification Regime. Sarah joined Ropes & Gray in 2018 from a magic circle firm in London.

Abraham Lee
Ropes & Gray LLP

Abraham Lee is an associate at Ropes & Gray's New York office and is a member of the firm's litigation department.

© Law Business Research 2021

Nico Leslie
Fountain Court Chambers

Nico Leslie is a member of Fountain Court Chambers, London.

He was called to the Bar in 2010 and has since developed a practice involving both national and international disputes. In particular, he has done significant work in Singapore, both in arbitration and before the newly formed Singapore International Civil Court.

Nico's practice comprises mainly complex financial and civil fraud litigation, having acted in some of the largest UK disputes of recent years, including the *Sebastian Holdings*, *Algosaibi*, *Gemini* and *Republic of Djibouti* cases. In light of this experience, Nico was recently identified as one of 10 junior 'Stars at the Bar' by the UK legal press.

Nico is the co-author (with Marcus Smith QC) of *The Law of Assignment* (published by OUP), one of the leading texts on the creation and transfer of intangible property. He has also been commissioned by OUP (with Marcus Smith QC) to write a further book: *Private International Law and Intangible Property*. Nico speaks fluent French, Italian and Serbo-Croat and is comfortable working in those languages.

Megan Y Lew
Cravath, Swaine & Moore LLP

Megan Y Lew is a practice area attorney in Cravath's litigation department. Her practice focuses on internal and government investigations, civil litigation and regulatory compliance, including matters concerning the FCPA, fraud, money laundering and anti-money laundering controls, trade sanctions and export controls.

Jason Linder
Mayer Brown

Jason Linder, a former senior federal prosecutor, co-chairs Mayer Brown's global anti-corruption and FCPA practice. Resident in the firm's Washington and Los Angeles offices, Jason is a trial lawyer who counsels and defends boards, multinational companies and executives through corporate crises and government and media scrutiny; leads internal and government-facing investigations; and provides compliance counselling. Jason has led matters in more than 65 countries and in all major industries, and has deep expertise in corruption, securities fraud and other financial fraud, money laundering, tax evasion and anticompetitive conduct.

Jason is highly regarded by US and foreign authorities. He has worked with or against nearly every major US Attorney's Office, many components of the DOJ's Main Justice, the Securities and Exchange Commission, other US law enforcement and regulatory agencies, and foreign authorities and multilateral development banks across the globe. Before joining Mayer Brown, Jason chaired another major firm's global investigations and white-collar criminal defence practice. From 2007 to 2017, he served as a federal prosecutor, both in the Department of Justice's Criminal Division – where he led many of the Department's cutting-edge international white-collar investigations – and as an Assistant US Attorney in the Southern District of Florida.

© Law Business Research 2021

James P Loonam
Jones Day

James Loonam is a partner at Jones Day in New York City, where he regularly advises companies and their senior executives in sensitive investigations and government enforcement actions. Prior to joining Jones Day, James was an Assistant US Attorney for the Eastern District of New York and Deputy Chief of that office's business and securities fraud section. James graduated from the University of Connecticut School of Law with honours, where he was a member of the Law Review.

Andrew Love
Cooley LLP

Andrew Love is an associate in the litigation team in Cooley's London office. Andrew has worked on a wide range of white-collar matters, with particular focus on international internal investigations. Andrew has also assisted corporate and individual clients in relation to investigations carried out by the SFO and FCA. Before joining Cooley, Andrew's experience included undertaking a review of the mis-selling of financial products by a global bank before the 2008 financial crisis.

Rebecca Loveridge
Fountain Court Chambers

Rebecca Loveridge is a barrister practising from Fountain Court Chambers who specialises in all areas of commercial law, including civil and regulatory proceedings relating to financial services. She is regularly instructed on matters concerning privilege and appeared as junior counsel for the Bar Council in *R (on the application of Prudential and another) v. Special Commissioner of Income Tax and another* [2013] UKSC 1, for ENRC in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2019] 1 WLR 791, for the Financial Reporting Council in *FRC v. Sports Direct plc* [2020] 2 WLR 1256, *A v. B and FRC* [2020] 1 WLR 3989 and *FRC v. Frasers Group plc* [2020] EWHC 2607 (Ch) and for Barclays Bank in *PCP Capital Partners LLP v. Barclays Bank plc* [2020] EWHC 1393 (Comm). She is also a contributor to the latest edition of *The Law of Privilege*, published by Oxford University Press.

Joanna Ludlam
Baker McKenzie LLP

Joanna Ludlam, a partner in the Baker McKenzie dispute resolution team based in London, leads the market-leading regulatory, public and media law team and co-chairs the firm's global compliance and investigations group.

Joanna advises clients in the areas of corporate investigations, administrative and public law, procurement law and litigation. She has particular expertise in the healthcare, technology and energy, mining and infrastructure sectors. Joanna handles all kinds of high court litigation as well as investigations, including issues of bribery, corruption and

© Law Business Research 2021

fraud. She advises clients, frequently at board level, on regulatory compliance and crisis and reputation management.

Joanna has been recognised by several industry directories and has won numerous awards for her work. She has been named one of *The Lawyer*'s Hot 100 for her practice, recognised by *Who's Who Legal* as a Future Leader of Legal Investigations and described as having an 'excellent reputation within the market', ranked by *Chambers and Partners* with commentators saying she is 'excellent, knowledgeable and well connected', and acknowledged by the *Financial Times* as a Champion of Women in the annual FT HERoes awards.

Vanessa McGoldrick
Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Vanessa McGoldrick is an associate in Skadden's government enforcement and white-collar crime group in London. She advises clients on a broad range of compliance and regulatory issues, including bribery, corruption and money laundering, fraud, compliance matters, and EU and UK sanctions. Her experience includes representing clients in civil and criminal law investigations and proceedings before a range of regulators, including the SFO, FCA, HMRC, CMA and OFSI, and advising clients facing parallel investigations and proceedings before the US Department of Justice, the US Securities and Exchange Commission, the French Parquet National Financier and various other international regulators.

Claire McLeod

Claire McLeod is the head of litigation, investigations and enforcement for Europe and the Middle East at Barclays. Prior to joining Barclays in 2013, Ms McLeod was at Simmons & Simmons LLP.

Michael McGovern
Ropes & Gray LLP

Michael McGovern is co-chair of Ropes & Gray's global government enforcement group, concentrating his practice in the areas of white-collar criminal defence and complex civil litigation, with a particular focus on investigations and prosecutions by the US Department of Justice, and the Securities and Exchange Commission of alleged violations of the federal antitrust laws, the federal securities laws (including the Foreign Corrupt Practices Act), and alleged violations of various healthcare laws and regulations (including the False Claims Act). Michael has over 25 years of experience representing domestic and multinational corporations and partnerships, board committees, and their officers, directors and other executives in complex criminal and civil investigations and litigation. Michael is also an accomplished criminal trial lawyer and has successfully defended clients in a wide variety of high-profile and sensitive matters. Michael is listed in The National Trial Lawyers Top 100 Criminal Defense Trial Lawyers – New York, *Benchmark Litigation*, *Chambers Global, The Legal 500* and *The Best Lawyers in America*.

© Law Business Research 2021

Prior to joining Ropes & Gray, Michael served for over seven years as an Assistant United States Attorney in the US Attorney's Office for the Southern District of New York, where he held supervisory positions in both the organised crime and terrorism unit and the general crimes unit.

Nick Marshall
Linklaters LLP

Nick Marshall is a managing associate in Linklaters' employment and incentives team. Having worked in both the United Kingdom and Singapore, he has a broad international practice, and advises clients on their most sensitive, complex and high-value people-related matters.

With increased regulatory activity across a number of sectors in recent years, Nick regularly advises clients on conducting internal investigations and engaging with regulators in contentious situations, often in relation to concerns raised by whistleblowers. He also provides training and advice on speaking up policies and arrangements to clients across a range of sectors (particularly in financial services), and acts for employers in defending legal claims by current and former employees relating to whistleblowing.

Julia Maskell
Cooley LLP

Julia Maskell is an associate in the litigation department in Cooley's London office. She works with companies on a range of matters, including international internal investigations, compliance, regulatory investigations and commercial disputes. She has experience in working with companies across Cooley's global platform in a range of industries, with a particular focus on manufacturers of consumer products.

Rita Mitchell
Willkie Farr & Gallagher LLP

Rita Mitchell is a partner in Willkie's compliance, investigations and enforcement and white-collar defence practices in London. Dual-qualified in the United States and the United Kingdom, her practice includes advising and defending corporations in a variety of criminal and civil investigation and enforcement matters, conducting complex, worldwide internal investigations relating to bribery, corruption and fraud, advising on and developing and benchmarking compliance programmes, conducting pre-merger and third-party due diligence, and providing day-to-day counselling and training on compliance with anti-corruption laws, including the US Foreign Corrupt Practices Act and UK Bribery Act 2010. Rita is the co-leader of the London Chapter of the Women's White Collar Defense Association, and has been recognised as 'a highly regarded name' and an 'up-and-coming star' in the financial crime investigations space.

© Law Business Research 2021

Ben Morgan
Freshfields Bruckhaus Deringer

Ben Morgan is a member of Freshfields' global investigations practice in London and a member of the corporate crime group. Ben joined the firm as a partner in 2017. He advises clients on identifying and controlling the risks that arise from regulatory and criminal law enforcement within the domestic and international landscape. Ben practised as a defence lawyer in the City of London before becoming a board member and the joint head of bribery and corruption at the UK Serious Fraud Office (SFO). There, he led some of the SFO's most significant corporate cases and influenced UK policy matters such as the introduction of deferred prosecution agreements, enforcement of the UK Bribery Act and development of the law of corporate criminal liability. He also had a particular focus on building the international relationships necessary to investigate and conclude the most complex matters.

David Mortlock
Willkie Farr & Gallagher LLP

David Mortlock is a partner and chair of the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. David provides clients with guidance on compliance and enforcement on national security-related issues, including sanctions and export controls, anti-money laundering and the Committee on Foreign Investment in the United States.

He helps clients to build and implement compliance programmes, conduct internal investigations, respond to government enquiries and address enforcement actions. From October 2013 to November 2015, David was director for international economic affairs at the White House National Security Council, where he was responsible for coordinating inter-agency work on sanctions, anti-corruption and other illicit finance issues. From August 2009 to October 2013, he held a number of roles at the US Department of State, including attorney-adviser for sanctions and terror finance, and deputy coordinator for sanctions policy.

David was centrally involved in developing or easing the sanctions programmes for Russia, Iran, Cuba, Burma and Venezuela, among others.

Christopher J Morvillo
Clifford Chance US LLP

Christopher J Morvillo has extensive experience representing corporate and individual clients in criminal investigations and proceedings, internal investigations, and related regulatory and civil matters. With a particular focus on cross-border government and internal investigations, his many representations have involved allegations of accounting fraud, public and foreign corruption, securities fraud, insider trading, economic sanctions violations, trade secret theft and computer fraud. Mr Morvillo also advises corporations and businesses on related compliance and policy matters.

From 1999 to 2005, Mr Morvillo served as an Assistant US Attorney for the Southern District of New York, where he investigated, tried and handled appeals in a wide variety

© Law Business Research 2021

of criminal cases, including in the area of healthcare fraud, insurance fraud, money laundering, obstruction of justice, counterterrorism and narcotics. In 2005, he received the US Attorney General's Award for Exceptional Service – the Department of Justice's highest award for prosecutors – in recognition of his role in the investigation and successful prosecution of a large international terrorism case.

Mr Morvillo was named one of the top five most highly regarded lawyers in the United States for business crime corporate defence in the 2016 edition of *Who's Who Legal*. Mr Morvillo's expertise has also been recognised by numerous other publications, including *Chambers*, *Best Lawyers in America* and *Super Lawyers New York*. Mr Morvillo speaks and writes frequently on government investigations.

Britt Mosman
Willkie Farr & Gallagher LLP

Britt Mosman is a partner in the global trade and investment group at Willkie Farr & Gallagher LLP in Washington, DC. Britt has advised global financial institutions and leading multinational companies on complex, international compliance and enforcement matters, particularly economic sanctions, anti-money laundering and anti-corruption laws, as well as transaction reviews by the Committee on Foreign Investment in the United States. Britt has deep experience with economic sanctions laws and regulations, having served as an Attorney-Advisor in the Office of the Chief Counsel (Foreign Assets Control) advising the Treasury Department's Office of Foreign Assets Control, prior to joining Willkie. In this capacity, she focused on economic sanctions and national security issues, including as a lead attorney on the Iran, Ukraine/Russia, Cuba, Syria election interference and cyber-related sanctions programmes.

David Murphy
Fox Williams LLP

David Murphy is a partner at Fox Williams LLP who specialises in guiding HR directors, boards and in-house legal teams through difficult employment situations, and in advising senior individuals when they join and leave their employers or face problems during their employment.

His corporate client base is focused on the financial services and professional services sectors, and he is experienced in advising on sensitive investigations in both sectors, particularly in respect of allegations relating to breaches of duty and conduct rules, and discrimination and harassment. His individual clients include fund managers, investment bankers, directors of listed companies and lawyers. He has advised several individuals at executive committee level on their departures from a major bank. In the 2020 edition of *The Legal 500*, David is recognised as a 'superb commercially astute employment law partner. His advice is pragmatic and tailored to a deep understanding of our business needs'. In the 2021 edition of *Chambers and Partners*, he is described as 'excellent technically, approachable, commercially astute, pragmatic, flexible and responsive'.

© Law Business Research 2021

Aisling O'Sullivan
Brown Rudnick LLP

Aisling O'Sullivan is an associate in Brown Rudnick's white-collar crime group. Her practice focuses on compliance, corporate crime, investigations and civil litigation, including asset-tracing and recovery. Aisling provides advice and representation to corporates and individuals facing criminal and regulatory enforcement action. She has acted on investigations led by UK and international agencies into allegations of fraud, bribery and corruption, false accounting and money laundering. Aisling also has experience in requests for mutual legal assistance and extradition, relating to the investigation and prosecution of criminal offences abroad.

Tamara Oppenheimer QC
Fountain Court Chambers

Tamara Oppenheimer QC has been practising as a barrister at Fountain Court Chambers since 2002, having previously trained and worked as a solicitor in the litigation department at Allen & Overy. She was appointed Queen's Counsel in 2020. She has a broad commercial litigation practice spanning financial services, regulatory, general commercial disputes, professional negligence, insurance and aviation. She is a contributor to *The Law of Privilege*, edited by Bankim Thanki QC, and co-author of the chapter on privilege in *Lissack and Horlick on Bribery* (Third Edition, 2020). Tamara is regularly instructed on matters concerning privilege and confidentiality, particularly in the regulatory and investigatory context. She has appeared in a number of leading privilege cases, including *Dechert v. Eurasian Natural Resources Corporation* [2016] 1 WLR 5027; *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205 (at first instance) and [2019] 1 WLR 791 (in the Court of Appeal); and *R (on the application of Jet 2.com) v. Civil Aviation Authority* [2020] 2 WLR 1215.

Simon Osborn-King
Willkie Farr & Gallagher LLP

Simon Osborn-King is a partner in Willkie's litigation and compliance, investigations and enforcement practices in London. Simon has a broad-ranging domestic and cross-border investigations, commercial litigation and arbitration practice. Simon has significant experience in complex regulatory, criminal and internal investigations and enforcement proceedings facing multinational corporations, financial institutions and individuals across a wide spectrum of business sectors. Simon has defended clients before the UK Financial Conduct Authority and Serious Fraud Office, the US Department of Justice, the European Commission, Italy's Public Prosecutors' Office, the Japan Financial Services Agency and the Korea Fair Trade Commission. Simon was recognised in the 2020 edition of *Global Investigations Review*'s '40 under 40', which celebrates the next generation of leading investigations specialists from around the world.

© Law Business Research 2021

Jeel Oza
Ropes & Gray LLP

Jeel Oza is an associate in Ropes & Gray's Washington, DC, office and is a member of the firm's litigation department.

Jessica Parker
Corker Binning

Jessica Parker is a specialist in investigations and criminal and regulatory litigation. Jessica has experience representing businesses and executives in investigations by all of the major prosecuting agencies. She has particular expertise in international investigations, including international requests for evidence and asset freezing. Case highlights include acting for the former chief executive of Barclays Bank who was acquitted following his trial in connection with the SFO's investigation into the 2008 capital raising; representing senior figures who were not charged in several significant SFO investigations, including Rolls-Royce, G4S and Serco; conducting an investigation on behalf of a founder in respect of a major fraud allegation also under investigation by the SFO; and representing senior executives in HMRC investigations into tax fraud and defending in HMRC's longest running and most complex tax case (Operation Amazon).

Avni P Patel
Walden Macht & Haran LLP

Avni Patel is an experienced litigator and trial attorney who has represented individuals and corporate clients in complex, sensitive and high-profile cases including in federal, state, and local criminal and regulatory matters. Her practice focuses on white-collar criminal defence, government investigations and regulatory enforcement, and complex litigation. At Walden Macht & Haran (WMH), Avni was part of the trial team who successfully defended a corporate client in a high-profile public corruption case in the Southern District of New York. They won the only acquittal in the highly contested and publicised four-defendant trial. She also is part of the WMH team representing one of the most significant whistleblowers in sports history. Additionally, Avni was on the leadership team of the independent monitor named by the US Department of Justice to oversee General Motors' compliance with its obligations under the deferred prosecution agreement stemming from its recall of defective ignition switches. Before joining WMH, Avni served as an Assistant District Attorney for five years in the Bronx County District Attorney's Office. In those five years, Avni tried over 15 felony and misdemeanour cases to verdict – five of them to jury verdict – on charges ranging from attempted murder to grand larceny. Avni is a graduate of Boston University School of Law and Northwestern University.

© Law Business Research 2021

Nichola Peters
Addleshaw Goddard LLP

Nichola Peters is a partner and heads up Addleshaw Goddard's global investigations and contentious regulatory group. She specialises in advising corporates, directors and senior management on regulatory inquiries, financial and corporate crime issues. Key areas involve advising on and carrying out investigations relating to corporate collapse, corruption, sanctions, money laundering, terrorist financing, extradition, information security and fraud issues. As Nichola regularly investigates compliance failings, she is able to provide specialist non-contentious advice on what to look out for, how matters can go wrong and how to minimise that risk. In relation to contentious matters, because Nichola works regularly with clients to conduct due diligence and implement effective compliance programmes, she has an excellent understanding of industry standard practice and what procedures should have reasonably been put in place to prevent compliance failings. Nichola is ranked as a Thought Leader in *Who's Who Legal: Investigations* and *Who's Who Legal: Business Crime Defence* and as a Leading Individual in *Who's Who Legal: Trade & Customs (International Sanctions)*. Nichola was selected by *Global Investigations Review* in 2018 as one of 100 remarkable women investigation specialists operating across the world. Nichola was also named as one of *The Lawyer*'s 'Hot 100' lawyers in 2017.

Hayley Pizzey
Latham & Watkins

Hayley Pizzey is an associate in the London office of Latham & Watkins and a member of the firm's litigation and trial department.

Ms Pizzey is a trusted adviser to a number of international organisations. She is frequently engaged in complex and high-value disputes and regulatory inquiries. Ms Pizzey primarily handles multi-jurisdictional litigation and regulatory matters. She advises clients on a wide range of disputes, with a particular focus on commercial litigation and contentious data protection as well as regulatory investigations.

Ms Pizzey's role includes advising on inquiries commenced by the Irish Data Protection Commission, compliance with the GDPR, alleged data breaches and regulatory notifications, and regulatory sanctions.

Ms Pizzey's experience includes claims in the High Court, the Court of Appeal and the Competition Appeal Tribunal. She has also acted on matters involving the Competition and Markets Authority, the European Commission, and numerous data protection authorities and financial services regulators around the world.

Ms Pizzey is also a trusted adviser to her *pro bono* clients.

Glenn Pomerantz
BDO USA, LLP

Glenn Pomerantz leads BDO USA LLP's global forensics practice with nearly 35 years of forensic accounting, auditing and consulting experience. Working with multinational organisations and their counsel, Glenn leads cross-border matters that mitigate the risks associated with fraud and corruption. He works with BDO leaders around the globe to

© Law Business Research 2021

respond to clients' needs involving anti-corruption and fraud investigations, forensic technology, compliance and due diligence matters in mature and emerging markets.

Glenn has significant experience in managing engagements involving alleged violations of the Foreign Corrupt Practices Act and UK Bribery Act, and embezzlement, theft and financial-reporting fraud. In addition, he has spent much of his career providing expert witness testimony on economic damages, as well as providing litigation and dispute advisory services, including evaluating claims under fidelity bonds and employee dishonesty insurance coverage. He has also served as a court-appointed umpire and referee and as a neutral arbitrator.

Alison Pople QC
Cloth Fair Chambers

Alison Pople QC is a barrister with over 25 years' experience, specialising in financial and commercial crime, and corporate crime and investigations. She acts for corporate clients and senior individuals in global investigations. Her expertise embraces the interface between the commercial world and criminal or regulatory investigations, including issues of corporate fraud, domestic and international corruption, tax fraud, money laundering, criminal cartels, insider dealing and corporate regulatory issues. She has worked on many high-profile and sensitive investigations in recent years. She is highly ranked as a leading silk in Financial Crime and Financial Crime (Corporates) in Chambers' *UK Bar* guide 2021 and described as 'tremendous'. She is listed by *Who's Who Legal* as a Thought Leader and a Global Leader in the fields of investigations, business crime individuals and business crime corporates for 2020 and a National Leader in *UK Bar: Criminal Fraud and Investigations* for 2020. She is described as 'a "top notch silk" who comes highly recommended by her peers for her deep experience in commercial criminal investigations'.

Elly Proudlock
Linklaters LLP

Elly Proudlock acts in investigations by the Serious Fraud Office (SFO) and other authorities, representing companies and individuals facing allegations of fraud, bribery and corruption, money laundering and other types of misconduct. Key work highlights for Linklaters include working on an SFO investigation for a multinational energy services company, representing a non-UK listed company in a self-report and acting for a UK-listed company in an SFO fraud investigation. Previous experience includes representing senior individuals in SFO investigations involving high-profile names such as Barclays, ENRC and Rolls-Royce. Elly also regularly advises companies on the whole range of issues relating to business crime, including anti-bribery and corruption and anti-money laundering. Elly is ranked in Band 4 in the 2022 edition of *Chambers UK* for Financial Crime: Corporates.

© Law Business Research 2021

Nicholas Purnell QC
Cloth Fair Chambers

Nicholas Purnell's practice in commercial and business crime and in regulatory and professional disciplinary matters has spanned over four decades. Typically instructed at the early stages of investigations pre-charge, he advises clients in cases under examination by global regulatory and prosecuting authorities including the Serious Fraud Office (SFO), the Financial Conduct Authority, the US Department of Justice and the Securities and Exchange Commission.

The development of collaborative investigations across jurisdictions has brought about the need for teams to be in place to provide joint advice on the impact of managing the response to investigations on a global basis. Nicholas has specialist experience in the development of the appropriate strategy to enable businesses to develop and cope with the resource demands imposed by such investigations.

Nicholas acted for ICBC Standard Bank throughout the first ever deferred prosecution agreement to be approved in the United Kingdom. Following months of negotiations with the SFO, Nicholas appeared before the President of the Queen's Bench Division at the High Court where the terms of the agreement were finalised. This case marked Nicholas's hat-trick of firsts: the first civil settlement with the SFO for Balfour Beatty; the first attempt at a simultaneous global settlement in the United States and the UK with the SFO in Innospec; and the combination of this first charge under section 7 of the Bribery Act in achieving this deferred prosecution agreement with the SFO.

Nicholas successfully represented clients in the United Kingdom over allegations made by the SFO against Tesco and Barclays and advised one of the three DePuy International executives who was on trial in Athens.

Amanda Raad
Ropes & Gray LLP

Amanda N Raad serves as a trusted adviser to clients seeking wide-ranging counsel on global and cross-border risk. Qualified in the United States, a US lawyer who is also admitted and as a solicitor in England and Wales, she leverages her extensive knowledge and experience of these active enforcement regimes to help clients navigate risk from both jurisdictions. As founder of Ropes & Gray's Data and Behavioral Science Initiative, Amanda is a leader in the use of data analytics and behavioural science to help organisations establish compliance-driven cultures, effectively manage global risk and implement remediation solutions as necessary. Her work addresses the full risk spectrum, encompassing financial fraud, corruption, sanctions, money laundering, cyber and data privacy risk, antitrust compliance and sexual misconduct.

Global co-leader of Ropes & Gray's anti-corruption and international risk practice, Amanda also co-founded the firm's fraud in times of crisis task force, as well as the firm's global health care compliance initiative. She publishes and speaks frequently on cross-border challenges in the areas of corporate crime and investigations, including those associated with sexual misconduct. She is a regular contributor to Global Investigations

© Law Business Research 2021

Review's (GIR) *The Practitioner's Guide to Global Investigations* and serves as a committee member for the American Bar Association's Women's White Collar Defense Association and the UK's Fraud Lawyers Association. Amanda is listed in GIR's *Women in Investigations* 2018, *Chambers UK*, *The Legal 500 UK* and *New York Super Lawyers*.

Samuel Rabinowitz
Fountain Court Chambers

Samuel Rabinowitz is a barrister practising from Fountain Court Chambers and specialising in commercial law. Sam is regularly instructed on matters concerning privilege, and as a pupil assisted counsel for ENRC in the trial of *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205. Sam worked as a judicial assistant in the Commercial Court for six months in 2018.

Pamela Reddy
Norton Rose Fulbright LLP

Pamela Reddy is a white-collar crime and investigations lawyer based in London. Pamela is widely recognised as one of the United Kingdom's most distinguished white-collar crime lawyers.

With more than 20 years' experience, Pamela is able to advise on the full spectrum of criminal and regulatory law and covers all stages of investigations, from the initial internal investigation and potential self-reporting, through to interviews under caution, all the way to defending clients in jury trials. She has also worked on several high-profile public inquiries and advised individuals facing sexual misconduct allegations, which surfaced amid the #MeToo movement.

Pamela is now a first-choice counsel to global companies and senior executives on domestic and cross-border fraud, bribery and corruption, market abuse and money laundering investigations. She frequently acts on some of the most serious, complex and high-profile cases involving UK and foreign regulators, including the SFO, NCA, CPS, FCA and DOJ.

Prior to joining the firm, she led a team at a boutique criminal law firm, advising on high-profile and media-sensitive general criminal matters and white-collar crime.

Pamela is recognised in *Financier Worldwide*'s 'Power Players in Investigations & White Collar Crime 2021', *Who's Who Legal*'s Global Leaders in Investigations 2020 and *Global Investigations Review* 'Top 100 Women in Investigations 2018'. Pamela features in the top tiers of a range of criminal law categories by the leading legal directories, in which she has been described as 'brilliant – she is extremely knowledgeable, has good technical skills and works tirelessly'.

© Law Business Research 2021

Andrew Reeves
Norton Rose Fulbright LLP

Andrew Reeves is a dispute resolution and investigations partner based in London. He works on a range of major regulatory and criminal investigations and related litigation, focusing on bribery and corruption, fraud, financial crime and money laundering.

Andrew advises corporates, financial institutions and senior executives on major investigations conducted by the UK Serious Fraud Office, Financial Conduct Authority and Prudential Regulation Authority, as well as the US Department of Justice and Securities and Exchange Commission and various regulators globally.

Andrew also has significant experience of designing and implementing compliance programmes and conducting transactional due diligence, internal investigations and related litigation for corporates and financial institutions, with a focus on multi-jurisdictional bribery and corruption, fraud and money laundering matters.

He regularly advises on money laundering reporting and defence suspicious activity reports, as well as multi-jurisdictional cannabis-related money laundering issues.

Andrew is recommended in *The Legal 500: Regulatory Investigations and Corporate Crime* 2020 and 2021 and described as 'outstandingly able and immensely practical'.

Charles D Riely
Jenner & Block LLP

Charles Riely is a partner at Jenner & Block and a member of its investigations, compliance and defence, markets and trading and securities litigation and enforcement practices. Before joining Jenner & Block, he served as a lawyer at the Securities and Exchange Commission (SEC) for more than a decade, most recently as assistant regional director for the SEC's Division of Enforcement. While with the SEC, he worked on matters involving disclosure failures by public companies, alleged fraud and regulatory violations by investment advisers and broker-dealers, insider trading, anti-money laundering violations, 'spoofing' and other forms of market manipulation, failure-to-supervise violations, the adequacy of firms' cybersecurity procedures and protections, and a variety of other fraud and regulatory matters. Mr Riely also coordinated investigations with the US Department of Justice and worked on more than a dozen publicly filed SEC enforcement actions in which criminal authorities filed a parallel case. He graduated from the University of Michigan Law School and served as a law clerk to the Hon Frank Maas of the US District Court for the Southern District of New York. He is admitted to practise in New York.

Cheryl Risell
Cadwalader, Wickersham & Taft LLP

Cheryl Risell is an associate in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. She advises clients in a broad range of criminal, civil and administrative proceedings and litigation. Her past experience includes commercial disputes, securities litigation and administrative law, as well as disputes arising under the Controlled Substances Act and federal securities regulations. In those roles, Cheryl

© Law Business Research 2021

has advised a variety of clients, including financial services firms, investment funds, large corporations and individual executives.

Cheryl received her undergraduate degree in international affairs and political science from Florida State University and a masters degree in politics and government of the European Union from the London School of Economics. She completed the GDL and LPC at the University of Law in London and also received a Master of Science in law, business and management. She is admitted to practise in England and Wales.

Patrick T Roath
Ropes & Gray LLP

Patrick Roath is an associate in Ropes & Gray's Boston office and is a member of the firm's litigation department.

Kevin Roberts
Cadwalader, Wickersham & Taft LLP

Kevin Roberts is a partner in Cadwalader's white-collar defence and investigations group, resident in the London office. He specialises in regulatory compliance and investigations and white-collar crime. Kevin's practice ranges from regulatory matters dealt with by the Financial Conduct Authority, Medicines and Healthcare Products Regulatory Agency, and the Health and Safety Executive, to prosecutions brought by the Serious Fraud Office. Kevin advises corporations and individuals on money laundering compliance and investigations; anti-corruption and regulatory compliance; asset-tracing and recovery; tax investigations; and fraud. As part of his global practice, Kevin advises clients on mutual assistance requests and extradition. He also counsels them on parliamentary select committee appearances.

Elizabeth Robertson
Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Elizabeth Robertson is a partner in Skadden's government enforcement and white-collar crime group in London. She advises on multi-jurisdictional business crime and regulatory matters around the world. Ms Robertson has played a role in many of the most important criminal and regulatory investigations in the United Kingdom over the past 20 years, giving her significant understanding of the priorities of the UK prosecuting authorities such as the SFO, the FCA, HMRC and the Competition and Markets Authority. She has particular experience in corruption, money laundering, economic sanctions and criminal tax cases. Ms Robertson has also advised on criminal cartel matters, and regularly assists with governance and compliance issues as well as proceedings brought by professional and regulatory bodies. She has successfully defended clients on enforcement actions brought by multiple agencies and responded to coordinated dawn raids in the UK and overseas. Ms Robertson also has experience in ancillary matters such as extradition and mutual legal assistance and applying to Interpol for access to information or for information to be amended or deleted.

She is also an accomplished speaker on international business crime.

© Law Business Research 2021

Ali Sallaway
Freshfields Bruckhaus Deringer

Ali Sallaway is co-head of Freshfields' global investigations and corporate crime practice in London, and she has been a partner at the firm since 2005. With a record of acting on significant cross-border and domestic investigations for clients in all sectors, Ali specialises in particular on corporate and financial crime defence and regulatory enforcement actions. She has significant expertise in handling fraud, false accounting, bribery and corruption, money laundering and terrorism matters as well as acting in relation to market abuse, disclosure and listing obligations for listed companies. Highlighted in *The Lawyer*'s Hot 100 for 2015, Ali is recognised as a leading individual in corporate crime, contentious financial services and investigations by all the major directories.

Richard Sallybanks
BCL Solicitors LLP

Richard Sallybanks, a partner in BCL for 20 years, has been involved in numerous UK and international business crime investigations and prosecutions.

His core practice is defending senior executives who are suspects in investigations. His SFO experience includes the Petrofac, Airbus, Barclays Qatar, Alstom and Kaupthing Bank investigations as well as successfully defending Tesco's commercial director on charges of an alleged £250 million accounting fraud. Many of his cases are cross-border, and Richard is experienced in managing and co-ordinating teams of lawyers in multi-jurisdictional investigations. In the financial sector he has acted for bankers, brokers, traders and senior executives in criminal and regulatory investigations, by the FCA and overseas authorities, including in relation to allegations of money laundering, insider dealing and market abuse. Many of his clients are high net worth individuals whom Richard advises in connection with business crime and tax investigations, as well as the implications of overseas criminal investigations, the mutual legal assistance regime, extradition and Interpol.

David Sarratt
Debevoise & Plimpton LLP

David Sarratt is a partner in Debevoise's litigation department. He is a seasoned trial lawyer whose practice focuses on government enforcement actions, internal investigations and complex civil litigation for financial institutions and other clients. Mr Sarratt has particular experience in matters relating to compliance with the Bank Secrecy Act and the FCPA, as well as with novel enforcement issues arising from new technologies.

Mr Sarratt has been recognised as a rising star by the *New York Law Journal* 2017, as a future star by *Benchmark Litigation* 2021 and as a next generation lawyer by *The Legal 500 US* 2018 for cyber law.

Prior to joining the firm, Mr Sarratt served as an Assistant United States Attorney in the Eastern District of New York. As a federal prosecutor, Mr Sarratt supervised and participated in a wide variety of investigations and prosecutions, involving international terrorism, cybercrime, financial and healthcare fraud, racketeering and other crimes. He

© Law Business Research 2021

successfully tried numerous cases to verdict and briefed and argued appeals in the US Court of Appeals for the Second Circuit.

Judith Seddon
Ropes & Gray LLP

Judith Seddon is global co-head of Ropes & Gray's white-collar and government enforcement practice.

Judith is a leading and consistently ranked Band 1 practitioner specialising in white-collar crime, fraud, money laundering, corruption, and regulatory and criminal investigations and prosecutions. She has successfully represented corporate clients, including leading financial institutions, in some of the most significant and complex investigations mounted by the Serious Fraud Office (SFO) and Financial Conduct Authority (FCA) in the United Kingdom and by prosecuting authorities across the globe. She has successfully represented individuals in a number of the highest-profile investigations. Judith has conducted numerous internal investigations for clients involving highly sensitive matters, successfully defended clients against threatened actions by the SFO and FCA and other government agencies, and guided clients through the myriad and often unexpected challenges of navigating cross-border investigations.

Judith's professional career began at a leading specialist criminal law practice in central London led by the late Rod Fletcher. She made partner there in 2002. In 2008, she moved to a magic circle firm, where she became director in 2011 and partner in 2014; she was one of the first criminal law practitioners to join a magic circle firm, as the need for specialist criminal practitioners to deal with the growth of investigations and prosecutions of white-collar crime became essential. She joined Ropes & Gray in 2018.

Described by *Chambers* as 'excellent' and by *Who's Who Legal* as 'sharp and clever', she is acknowledged by her peers, clients and the legal press as a thoroughgoing and trenchant litigator, with an eye for detail, yet strategic, committed and indefatigable in the representation of her clients.

Sean Seelinger
Ropes & Gray LLP

Sean Seelinger, a partner at Ropes & Gray in London, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

© Law Business Research 2021

Benjamin Sharrock
Cooley LLP

Benjamin Sharrock is an associate in the commercial litigation department of Cooley's London office. Benjamin advises on white-collar crime matters concerning companies and senior individuals in allegations of fraud, bribery and corruption and anticompetitive behaviour. He also advises on a broad range of complex contractual disputes and regulatory investigations across a variety of industry sectors and jurisdictions, often with a cross-border element. Benjamin has particular experience dealing with leading UK authorities, including the Serious Fraud Office.

Grace C Signorelli-Cassady
Jenner & Block LLP

Grace Signorelli-Cassady is an associate at Jenner & Block focusing on investigations, compliance and defence. Her experience includes assisting corporates in responding to government enquiries, including by US and European enforcement authorities; assisting corporates in conducting complex, worldwide internal investigations, including in connection with allegations of money laundering, bribery and corruption; and representing criminal defendants at trial and post-conviction, including individuals in white-collar matters, including for misrepresentations to investors and mail and wire fraud. She has also drafted nearly a dozen *amicus curiae* briefs regarding white-collar and criminal law issues, most of which were filed with the US Supreme Court. Prior to joining Jenner & Block, Ms Signorelli-Cassady served as a law clerk to the Hon Roslyn O Silver of the US District Court for the District of Arizona, during which time she assisted with matters taken by designation in the US Court of Appeals for the Ninth Circuit. Ms Signorelli-Cassady received her law degree from Harvard Law School, where she was the managing editor of the *Harvard Journal on Legislation*, selected as a criminal justice fellow and trained in negotiation techniques. She is admitted to practise in Illinois.

Daniel Silver
Clifford Chance US LLP

Daniel Silver is a partner at Clifford Chance US LLP, where he focuses on regulatory enforcement and white-collar criminal defence. Dan represents both individuals and corporations in matters before the Department of Justice and other federal and state enforcement agencies, and counsels clients on risk mitigation strategies with respect to cybersecurity, anti-corruption, sanctions and anti-money laundering issues. Prior to joining Clifford Chance, Dan spent 10 years as a federal prosecutor, serving in several senior leadership positions and overseeing the national security and cybercrime unit within the United States Attorney's Office for the Eastern District of New York. Dan received his undergraduate degree from Brown University and his JD, *magna cum laude*, from New York University School of Law.

© Law Business Research 2021

Alexander B Simkin
Ropes & Gray LLP

Alexander Simkin is counsel in Ropes & Gray's New York office. Alex is a trial lawyer and problem-solver who represents corporate clients through all stages of complex commercial litigation, from pre-litigation advisory services to trial and appeal. He has tried cases before juries, judges and arbitrators on behalf of plaintiffs and defendants and has appeared in federal and state courts across the United States. He devotes a significant part of his practice to representing financial institutions, including those involved in private equity, banking, insurance and other financial services.

Ilana Sinkin
Norton Rose Fulbright LLP

Ilana Sinkin is a senior associate in Norton Rose Fulbright's Washington, DC, office, where she focuses her practice on regulatory and government investigations, white-collar criminal defence, compliance and internal investigations for both corporations and individuals. Ilana has experience in a broad range of government and internal investigations, including investigations related to anti-corruption laws such as the US Foreign Corrupt Practices Act and the UK Bribery Act, sanctions and export control, securities enforcement, insider trading, financial fraud, the False Claims Act and market manipulation.

Ilana also has experience designing anti-corruption compliance policies and procedures, designing investigative plans, preparing witnesses for interviews, assisting in document collections and productions, managing document reviews, preparing investigative reports, responding to subpoenas and participating in presentations to enforcement authorities, including the Department of Justice, the Office of Foreign Assets Control, the Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Department of Commerce, Bureau of Industry and Security.

Ilana is admitted to practise law in Virginia and the District of Columbia. She is also admitted to practise in the United States District Court in the Eastern District of Virginia.

Andrew Smith
Corker Binning

Andrew Smith specialises in business crime, including SFO, NCA and police investigations relating to fraud, bribery and corruption, and money laundering, as well as regulatory inquiries brought by the FCA into market abuse and market misconduct. Andrew also regularly acts for individuals facing extradition to a range of countries and provides related advice on Interpol and criminal mutual legal assistance. Case highlights include acting for individuals in SFO investigations, including Tesco, BAT, Petrofac, Unaoil, LIBOR and EURIBOR; representing a defendant in the FCA's largest prosecution of insider dealing (Operation Tabernula) and FCA regulatory investigations concerning LIBOR and FX; advising businesses on alleged breaches of export controls and trade and financial sanctions; acting for executive counsel to the Financial Reporting Council on disciplinary investigations into major firms of accountants; and representing Shrien Dewani in the South African request for his extradition for the offence of murder.

© Law Business Research 2021

Meghan K Spillane
Goodwin

Meghan Spillane, a partner in Goodwin's securities litigation and white-collar defence group, focuses her practice on white-collar criminal defence, corporate internal investigations, and complex business and financial litigation. Her experience includes federal criminal and civil investigations, securities class actions and derivative suits, SEC actions, and complex civil litigation matters. In addition to her other client work, Ms Spillane represents indigent criminal defendants on a *pro bono* basis in a variety of state and federal matters. Ms Spillane is a member of the bar of the State of New York and is admitted to practise before the US District Court for the Southern District and Eastern District of New York. Ms Spillane was named as a 2018 *Law360* Rising Star in 'White Collar', was recognised in *Who's Who Legal: Investigations – Future Leaders* 2019 and has been named consistently by *New York Super Lawyers* as a leading white-collar defence practitioner (2015–2021). She was also recognised by *Benchmark Litigation*'s '40 & Under Hot List' for 2020 and 2021 for her work in white-collar defence.

Brian Spiro
Herbert Smith Freehills LLP

Brian Spiro is recognised as a leader in his field by all of the independent legal directories. A partner in the corporate crime and investigations team of Herbert Smith Freehills in London, Brian specialises in high-loss business crime litigation, fraud and regulatory matters, and has expertise in international law, including mutual legal assistance in criminal matters, overseas corruption and corporate investigations.

After a period as a parliamentary adviser, Brian trained as a solicitor with Clifford Chance and Simons Muirhead & Burton, London, qualifying as a solicitor in 1984.

Brian was a member of the Law Society's subcommittee and chair of the London Criminal Court Solicitors' Association subcommittee responding to the UK government's proposals on fraud law reform. He is lead author of *Police Station Adviser's Index* (Sweet & Maxwell), now in its fourth edition, and has acted as an international consultant to the WHO, the UN and the British Council on criminal law matters.

Brian is a former chair of the Business Crime Committee of the International Bar Association, a current member of Global Investigations Review's editorial board, and a regular writer and commentator on financial crime and related issues.

Daniel L Stein
Mayer Brown

Daniel Stein is a partner in Mayer Brown's New York office, leader of the global regulatory and investigations group and co-leader of the white-collar defence and compliance group. Dan focuses on representing and counselling financial services firms. He has extensive experience in regulatory enforcement, government and internal investigations, white-collar criminal defence and complex civil litigation. He counsels corporate and individual clients in a range of complex issues, including US Securities and Exchange Commission, and Financial Industry Regulatory Authority investigations and enforcement actions.

© Law Business Research 2021

Dan was chief of the Criminal Division for the US Attorney's Office for the Southern District of New York (SDNY), where he oversaw all of the SDNY's criminal prosecutions and investigations. He assumed that position in 2015, after serving as chief counsel to the US Attorney. From 2009 to 2011, he served as chief of the public corruption unit. Dan's decade-long career with the US Attorney's Office in New York began in 2003, where, as an Assistant US Attorney, he investigated and prosecuted cases involving a wide range of federal crimes. Earlier in his career, Dan clerked for the Hon Leonard B Sand of the United States District Court for the SDNY.

Katie Stephen
Norton Rose Fulbright LLP

Katie Stephen is a financial services and investigations partner based in London. She specialises in advising clients on contentious regulatory matters, including internal and external investigations and enforcement proceedings involving a variety of regulators including the FCA, PRA, SFO, HMRC and Ofgem, as well as those in other jurisdictions.

She has twice been seconded to the FCA as a legal adviser to its Regulatory Decisions Committee and she has acted on a number of high-profile cases, including market abuse proceedings against firms and individuals. Katie has also conducted a wide range of internal investigations for financial institutions and corporates, including advising on the regulatory implications and cross-border issues arising from these, and she is praised by clients for her 'investigatory talents' (*The Legal 500*).

Richard M Strassberg
Goodwin

Richard Strassberg, chair of Goodwin's white-collar crime and government investigations practice and a former member of the firm's executive committee, specialises in white-collar criminal defence, SEC enforcement proceedings, FCPA compliance and investigations, internal investigations, and complex business and financial litigation. Mr Strassberg is the chair of the downstate NY committee of the American College of Trial Lawyers, one of the premier legal associations in America. He has twice been recognised by *The American Lawyer* as 'Litigator of the Week' as a result of his securing extraordinary victories in some of the most closely followed white-collar trials in the country. He is also acknowledged by his peers as being one of the finest white-collar attorneys, twice being cited in *Law360* by white-collar partners at other firms as being the white-collar lawyer that impressed them, or that they most feared to go up against in court. In 2021, he was honoured as the White Collar Lawyer of the Year in New York by *Best Lawyers of America*. Mr Strassberg is consistently ranked in Band One by *Chambers USA* as among the top New York-based white-collar defence lawyers, is rated as being among the Top 100 lawyers in New York by *New York Super Lawyers* and is regularly included in *The Best Lawyers in America* and other surveys of the top white-collar litigators in the country. Mr Strassberg co-authors a quarterly column on Federal Civil Enforcement in the *New York Law Journal*, authored a chapter in the book *Beyond A Reasonable Doubt*, has published numerous articles in various legal periodicals, including several on the FCPA, has been a legal commentator

© Law Business Research 2021

on numerous programmes, including NPR, Fox News, Dateline and the Financial Management Network, and has been a guest speaker for various organisations, including the American Bar Association, the New York Council of Defense Attorneys and the Federal Bar Council. Prior to joining the firm, Mr Strassberg was the chief of the major crimes unit in the US Attorney's Office for the Southern District of New York, responsible for supervising approximately 25 Assistant US Attorneys in the prosecution of complex white-collar criminal cases.

Alex Swan
BCL Solicitors LLP

Alex Swan is a senior associate at BCL and specialises in corporate and financial crime. Alex has extensive experience of advising individuals and corporates at all stages of domestic investigations and prosecutions conducted by the SFO, the CPS, HMRC, the NCA and the FCA, and is well versed in mutual legal assistance, restraint and confiscation proceedings. His SFO experience includes the Airbus, GSK, HP/Autonomy and Rolls-Royce investigations as well as successfully defending Tesco's commercial director on charges of an alleged £250 million accounting fraud. His work regularly encompasses complex cross-border matters and he is experienced in dealing with matters investigated by a range of overseas authorities, such as those in France, India, Nigeria, Ukraine and the United States.

Lisa Tenorio-Kutzkey
DLA Piper LLP

Lisa Tenorio-Kutzkey (LT-K) focuses exclusively on white-collar matters in all phases of US federal government prosecution and investigation, with a focus on criminal antitrust defence, FCPA and complex internal investigations.

Lisa is a leader of DLA Piper's global cartel practice, a former trial attorney with the US Department of Justice's Antitrust Division and a former Special Assistant US Attorney for the US Attorney's Office for the Northern District of California. Fortune and Global Fortune 100, 200 and 500 companies and their executives routinely turn to Lisa for assistance in price-fixing, bid rigging and market allocation conspiracy matters. For more than a decade, she has successfully prosecuted or defended clients in nearly every major criminal cartel investigation by the Antitrust Division. Lisa has represented companies and individuals in a variety of sectors, including the automotive, aircraft and ocean transportation, telecommunications, semi-conductors, pharmaceuticals, construction, chemicals, industrial products, real estate and technology, and other electronic components industries.

In addition, Lisa has extensive experience in all facets of FCPA investigations, defence and compliance. She has directed and conducted cross-border investigations of FCPA and other anti-corruption and related compliance matters. Her practice is global in scope, with experience in Argentina, Belize, Brazil, Canada, Chile, China, Costa Rica, Ghana, Honduras, Hong Kong, India, Korea, Mexico, the Philippines, Russia, Thailand and Venezuela.

© Law Business Research 2021

Femi Thomas
Booking.com

Femi Thomas is chief compliance officer at Booking.com and formerly vice president and global head of ethics and compliance investigations at Nokia. Femi is a US-qualified attorney who, prior to joining Nokia in April 2017, worked in the white-collar and regulatory enforcement practice at Crowell & Moring LLP, Washington, DC, and then at Weatherford International in both legal and compliance roles and executive business roles. Femi has a juris doctorate degree and holds an executive MBA from the University of Oxford.

Andrew Thornton-Dibb
McGuireWoods

Andrew Thornton-Dibb is an English qualified attorney in McGuireWoods' Washington, DC, office and practises in the government investigations and white-collar litigation group as an international attorney. Andrew advises clients on internal investigations, and on criminal and regulatory issues, including authorities' investigations and prosecutions on both sides of the Atlantic. He is, and in the recent past has been, involved in representing clients in relation to enforcement authorities' investigations into UK Bribery Act offences, leading an internal investigation into allegations of a complex financial products fraud, and on various investigations being conducted by the DOJ, the SEC and the other US regulatory authorities. Andrew has experience in leading internal investigation teams, managing document reviews, conducting witness interviews, preparing investigation reports, advising clients on arrests and the execution of warrants and dawn raids, representing clients in interviews before authorities, advising on authorities' investigative powers, preparing formal reports to enforcement authorities, and interacting and negotiating with enforcement authorities in the resolution of criminal investigations.

Francesca Titus
McGuireWoods

Francesca Titus represents companies and individuals in complex, high-value, multi-jurisdictional white-collar crime litigation, often involving cybercrime. Francesca advises business leaders at times of crisis, when they are caught up in high-stakes investigations, prosecutions or security incidents. Francesca often works across borders, leading teams from around the globe to ensure a cogent worldwide strategy.

Her practice encompasses the full range of corporate crime, including computer-based offences, bribery and corruption, money laundering, fraud, tax evasion and insider dealing. She advises on investigations conducted by the Serious Fraud Office, Her Majesty's Revenue and Customs, the Financial Conduct Authority, the National Crime Agency and the Information Commissioner's Office.

An experienced barrister, she has defended clients in over 100 jury trials and appeared as advocate in the Court of Appeal (Criminal Division). She is based in the London office of McGuireWoods London LLP.

© Law Business Research 2021

Luke Tolaini
Clifford Chance

Luke Tolaini is a partner in Clifford Chance's international investigations practice. He has over 20 years' experience of investigations – many of these matters involving cross-border enforcement and related litigation. His domestic focus has been on matters involving the UK's Serious Fraud Office, Financial Conduct Authority and Competition and Markets Authority – including negotiating one of the 12 DPAs agreed to date in the United Kingdom – while his international practice has frequently involved engaging with US, European and Asian authorities on matters involving corruption, fraud, cartels, money laundering and market irregularities. He is also a lead partner in Clifford Chance's risk team, advising clients on the management and prevention of business conduct risk and crisis management. He is a member of the editorial board of Global Investigations Review.

Anne M Tompkins
Cadwalader, Wickersham & Taft LLP

Anne M Tompkins is a partner in Cadwalader's white-collar defence and investigations group, resident in the Charlotte, North Carolina, and Washington, DC, offices, and a member of the firm's management committee. Her practice focuses on representing companies and financial institutions, as well as their officers and directors in criminal, civil and administrative investigations. Anne has extensive experience in crisis management, internal investigations and enforcement matters across a variety of industries, including financial services, higher education and government contracting.

Anne was the United States Attorney for the Western District of North Carolina from April 2010 to March 2015. She led numerous high-profile, complex criminal and civil investigations during her tenure, including a public corruption case involving the former mayor of Charlotte, the national security case against former general and CIA director David Petraeus, numerous securities and financial fraud cases, and significant matters in the mortgage-backed securities business.

Prior to her service as US Attorney, Anne was a partner in the white-collar defence practice of a national law firm. In over 20 years' experience in government and private practice, Anne has tried more than 30 cases to verdict and successfully represented clients in, among other matters, investigations involving the mortgage practices of a national homebuilder, Medicare reimbursements to a cardiac care hospital, and anti-kickback and reimbursement compliance at a national dialysis services provider.

Serrin A Turner
Latham & Watkins

Serrin Turner is a partner in the New York office of Latham & Watkins, where he is a member of the firm's data privacy and security practice, white-collar defence and investigations practice, and complex commercial litigation practice.

© Law Business Research 2021

A former federal cybercrime prosecutor and experienced trial lawyer, Mr Turner represents technology companies and institutional clients in complex civil litigation, white-collar criminal defence matters, internal corporate investigations and crisis management situations, including data breaches and other cybersecurity incidents.

Matthew Valenti
Latham & Watkins

Matthew Valenti is an associate in the New York office of Latham & Watkins and a member of the firm's litigation and trial department. His practise focuses on white-collar defence and investigations, securities litigation, complex commercial litigation, and data privacy and cybersecurity issues.

Mr Valenti has represented individuals and corporations in a wide range of US government investigations led by the Department of Justice, the Commodity Futures Trading Commission, the Securities and Exchange Commission, and other regulatory agencies. He has also represented public and private companies in litigation in both federal and state court – including class actions alleging violations of US securities laws, and complex civil disputes implicating a broad spectrum of legal issues and industries. He also advises clients, both in regulatory inquiries and civil litigation, on data breach and data privacy matters.

Glenn K Vanzura
Mayer Brown

Glenn Vanzura is a partner in Mayer Brown's securities litigation and enforcement, and white-collar defence and compliance practices, resident in the Los Angeles office. He focuses his practice on securities litigation, complex business litigation, white-collar criminal defence and internal corporate investigations. Glenn has represented corporations, partners, directors, officers, employees and other individuals in a variety of industries, including the biopharmaceutical, semiconductor, medical service provider, automotive, real estate, casino gaming, hotel, smartphone application, entertainment, manufacturing and restaurant industries. He has also represented Am Law 100 law firms in legal malpractice and related matters and provided neutral party consultation to mediators in securities matters, particularly in respect of loss causation and damages issues. In recent matters, Glenn obtained a complete dismissal of a multimillion-dollar federal securities class action filed against a public company and its officers; persuaded the US Securities and Exchange Commission (SEC) to issue a 'no-action' letter for his corporate client under SEC investigation; convinced prosecutors threatening to indict his client and his client's corporation to forego any criminal charges; and first-chaired a successful civil arbitration in which his clients prevailed in a partnership dispute involving more than US$50 million in alleged damages.

© Law Business Research 2021

Johanna Walsh
Mishcon de Reya LLP

Johanna Walsh is a partner in the white-collar crime and investigations group. She has experience in domestic and international serious fraud, corruption and money laundering cases, acting for senior individuals in investigations and prosecutions brought by the Serious Fraud Office, the Financial Conduct Authority, the National Crime Agency, HM Revenue and Customs and the Crown Prosecution Service. Johanna has also acted for a range of corporates, from SMEs to FTSE 100 companies in relation to allegations of fraud and corruption, conducting internal investigations and representing them in external investigations and prosecutions. She has experience in negotiating deferred prosecution agreements and civil recovery orders.

Johanna is ranked in *Chambers and Partners* 2021 for Financial Crime, which notes that she is 'a very bright lawyer, dynamic, forthright with opponents and creative in her thinking'. She is named in *The Legal 500* in 2021 (Regulatory Investigations and Corporate Crime and for Fraud: White Collar Crime) and is a leading individual in Investigations and in Business Crime Defence (both Corporates and Individuals) in the 2020 edition of *Who's Who Legal*.

Holly Ware
Slaughter and May

Holly Ware, a partner in Slaughter and May's disputes and investigations group, has a broad practice that includes litigation and contentious regulatory and criminal investigations.

She has cross-jurisdictional investigation experience involving both regulatory and prosecuting authorities, including the LIBOR investigations and others relating to bribery and corruption, market abuse, money laundering and data breaches.

Anoushka Warlow
BCL Solicitors LLP

Anoushka Warlow is a senior associate specialising in acting for individuals in complex, multi-jurisdictional, allegations of serious fraud, bribery and corruption. She has been involved in many high-profile investigations and prosecutions brought by all the major domestic and international enforcement agencies. Her recent SFO experience includes acting for individuals in the ENRC, British American Tobacco, LIBOR and Standard Bank investigations, and she is currently representing several high net worth individuals who are the subject of investigations conducted by the SFO, HMRC and the US DOJ and SEC. Anoushka has expertise defending individuals in complex civil fraud proceedings and is also frequently asked to advise on the propriety of investigative steps taken by enforcement authorities, including asset freezing orders. She also has experience of challenging search warrants, production orders and the unlawful retention of evidence including through judicial review proceedings.

© Law Business Research 2021

Aaron Watkins
Cloth Fair Chambers

Aaron Watkins is a leading practitioner in the fields of extradition, mutual assistance, financial crime and cross-over criminal/public law matters. He regularly acts for defendants in the most high-profile and complex extradition cases before all levels of court. He has been instructed before the Supreme Court in the key cases under the Extradition Act 2003. Recent cases include the defences of individuals in the *HP v. Autonomy* proceedings, the Credit Suisse 'Tuna bond scandal' and the largest Scandinavian pensions fraud to date, spanning multiple jurisdictions. Aaron regularly acts for individuals facing politically motivated extradition requests from the Russian Federation, and recently successfully defended two individuals charged with fraud and bribery. Aaron has acted for requesting states in particularly high-profile cases, including for the Swedish authorities seeking the surrender of Julian Assange, for the Indian government in the successful extradition case concerning prominent businessman Vijay Mallya and for the US government in relation to the 'flash crash'. Aside from extradition, Aaron is a leading junior in the field of financial crime and related proceedings. He regularly acts for clients from investigation and initial advice through to trial and appeal. Most recently, Aaron successfully represented a client in obtaining the first-ever discharge of an unexplained wealth order.

Ella Williams
Slaughter and May

Ella Williams is senior counsel in Slaughter and May's disputes and investigations group. She has worked on some of the most complex, commercially sensitive multi-jurisdictional regulatory and criminal investigations of the past decade.

She advises corporations, financial institutions and individuals in relation to bribery and corruption, regulatory, tax and fraud investigations, including investigations and enforcement actions by the Financial Conduct Authority and Serious Fraud Office.

Mair Williams
Latham & Watkins

Mair Williams's practice focuses on white-collar defence. She has considerable trial experience, having started her career as a criminal barrister in chambers. She also has experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and develops compliance policies and practices for international clients.

In addition to her white-collar work, Ms Williams has experience in all manner of complex commercial litigation and has represented clients at every stage, from initial pleadings to trial and appeal. She has worked with clients representing a full spectrum of industries, including financial services, media, food and beverage, manufacturing and technology.

Ms Williams has conducted a range of internal investigations in jurisdictions around the world, including an investigation of a financial services firm following a leak of confidential information to the media, and an investigation on behalf of a private pension scheme following allegations made by a whistleblower. Her diverse range of representative

© Law Business Research 2021

experience includes representing a director in an investigation by the Financial Reporting Council into discrepancies with annual accounts of a FTSE 250 company and representing a publicly listed investment firm in investigations by the Financial Conduct Authority and Serious Fraud Office.

Ms Williams is a passionate *pro bono* advocate, and her practice is focused on representing individuals in the criminal justice system, particularly post-conviction.

Milton L Williams
Walden Macht & Haran LLP

Milton Williams's practice focuses on white-collar criminal and regulatory matters, employment law, litigation and advisory work representing corporations, and complex commercial litigation. He has litigated discrimination claims, Dodd-Frank and Sarbanes-Oxley retaliation claims, and SEC and IRS whistleblower claims on behalf of employees, and he has tried over 55 cases (civil and criminal) to verdict. Before joining Walden Macht & Haran, Milt served as deputy general counsel and chief compliance officer at Time Inc, where his responsibilities included compliance, the Foreign Corrupt Practices Act, OFAC and Sarbanes-Oxley, as well as intellectual property, privacy, data security and other cutting-edge areas. At Time Inc, Milt actively litigated a variety of employment law matters on behalf of the company concerning race, age and gender discrimination, and independent contractor litigation. In 2013, Milt was appointed co-chair of the Moreland Commission to investigate public corruption. Earlier in his career, Milt served as an Assistant US Attorney in the US Attorney's Office (USAO) for the SDNY. His last assigned unit in the USAO was the Securities and Commodities Fraud Force. He was also an Assistant District Attorney in the Manhattan District Attorney's Office. Milt is a graduate of Amherst College and the University of Michigan Law School in Ann Arbor.

Jason Williamson
Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Jason Williamson is an associate in Skadden's government enforcement and white-collar crime group in London.

He advises on the conduct of cross-border investigations into allegations of corporate misconduct, including fraud, corruption, money laundering, and other criminal and regulatory offences. His experience includes advising clients in relation to both civil and criminal proceedings, including actions commenced by the SFO, FCA, HMRC, CMA and US Department of Justice. He has also conducted cross-border investigations where allegations of civil wrongdoing have been made, including data privacy breaches.

He advises clients on anti-bribery and corruption matters and has successfully defended clients against enforcement actions commenced by multiple agencies. He regularly advises clients on governance issues, including compliance with EU and UK sanctions. He also has expertise in advising clients on the civil and criminal aspects of asset recovery and restraint proceedings.

© Law Business Research 2021

Alison Wilson
Linklaters LLP

Alison Wilson is global head of dispute resolution at Linklaters in London and a partner in Linklaters' Tier 1 contentious regulatory practice. She advises market-leading financial institutions, particularly in the retail bank sector, on their most significant FCA enforcement investigations, as well as on a range of internal investigations. She routinely advises firms on their investigation of whistleblowing concerns, including in an FCA enforcement context. She also has experience in advising clients under investigation by the SFO and overseas enforcement agencies.

Alison's extensive bank-sector knowledge has been supplemented by three bank secondments.

Zaneta Wykowska
Ropes & Gray LLP

Zaneta Wykowska is an associate at Ropes & Gray in London, who frequently assists a variety of multinational clients with conducting risk-based pre-acquisition deal diligence on cross-border transactions and advises on anti-corruption, anti-money laundering, sanctions, trade compliance and other regulatory issues associated with prospective business agreements.

Bruce E Yannett
Debevoise & Plimpton LLP

Bruce Yannett is deputy presiding partner of the firm, a member of the firm's management committee and chair of the white-collar and regulatory defence practice at Debevoise & Plimpton. He focuses on white-collar criminal defence, regulatory enforcement and internal investigations. He represents a broad range of companies, financial institutions and their executives in matters involving securities fraud, accounting fraud, foreign bribery, cybersecurity, insider trading and money laundering. He has extensive experience in representing corporations and individuals outside the United States in responding to inquiries and investigations.

Chambers Global 2021 and *Chambers USA* 2021 recognise Mr Yannett as a Band 1 practitioner for FCPA matters. He is also noted by *Chambers USA* 2021 as a leading lawyer for white-collar criminal defence and regulatory enforcement, by *Chambers Latin America* 2021 for corporate crime and investigations in Latin America, and by *The Legal 500 Latin America* 2021 for compliance and investigations in Latin America. Clients say 'he has tremendous credibility with boards and government agencies', he is 'one of the best-known and most able advisers for potential criminal issues with the government', and 'he has extremely deep knowledge, is very smart and strategic, and is a pleasure to work with'. They praise his work as 'excellent' and describe him as a 'very strong communicator and litigator' and a 'leading light in the field', noting that 'he has real gravitas about him', giving him the 'immediate respect of everybody in the room'. In a similar vein, he is recognised by *The Legal 500 US* 2021, which includes him in its 'Hall of Fame' and has called

© Law Business Research 2021

him a 'superstar', *Lawdragon* recognises him as one of the 500 leading lawyers in America, and *Benchmark Litigation* names him a 'Litigation Star'.

He is a member of the American Law Institute. Mr Yannett is on the board of advisers for the New York University programme on corporate compliance and enforcement.

Early in his career, Mr Yannett served in the Office of Independent Counsel: Iran/Contra and as an Assistant United States Attorney.

Steve Young

Association of Corporate Investigators

Steve Young spent 20 years in UK law enforcement with the City of London and Metropolitan police services investigating economic crime. He specialises in the proactive investigation of banking fraud, money laundering, bribery and corruption. He worked internationally with multiple law enforcement agencies in the United States, Europe and Asia. This was followed by six years as Citigroup EMEA regional director of investigations, and eight years as Barclays' global head of investigations for investment banking and wealth management. At Barclays, he managed a team of corporate investigators who worked globally on all aspects of internal and external economic crime, whistleblowing investigations, regulatory investigations and litigation support. To date, he has 41 years of international economic crime experience in both law enforcement and corporate environments. He speaks frequently on economic crime investigations at legal, corporate and law enforcement events. Steve is currently head of fraud and investigations at Lombard Odier & Co Ltd, based in Geneva, and chief executive officer of the Association of Corporate Investigators.

Yannis Yuen

Willkie Farr & Gallagher LLP

Yannis Yuen is an associate in Willkie's litigation, compliance, investigations and enforcement group in London. His practice involves advising on various aspects of white-collar crime, including bribery and corruption, tax evasion and sanctions, as well as modern slavery. He has experience advising in investigations and enforcement actions, including in front of the SFO, the FCA, the US Department of Justice and the Office of Foreign Assets Control. On the non-contentious side, Yannis also has experience in designing and implementing bespoke compliance programmes.

Jingxi Zhai

Cravath, Swaine & Moore LLP

Jingxi Zhai is an associate in Cravath's litigation department.

© Law Business Research 2021

Appendix 2

Contributors' Contact Details

ABB Ltd

Cityport
Affolternstrasse 44
8050 Zurich
Switzerland
Tel: +44 7342 089 528
tapan.debnath@gb.abb.com
https://global.abb/

Association of Corporate Investigators

Kemp House
152-160 City Road
London, EC1V 2NX
Tel: +44 20 3129 8522
steve.young@my-aci.com
www.my-aci.com

Addleshaw Goddard LLP

Milton Gate
60 Chiswell Street
London, EC1Y 4AG
United Kingdom
Tel: +44 20 7606 8855
nichola.peters@addleshawgoddard.com
michelle.dekluyver@addleshawgoddard.com
jaya.gupta@addleshawgoddard.com
www.addleshawgoddard.com

Baker McKenzie LLP

100 New Bridge Street
London, EC4V 6JA
United Kingdom
Tel: +44 20 7919 1000
Fax: +44 20 7919 1999
joanna.ludlam@bakermckenzie.com
mary.jordan@bakermckenzie.com

452 Fifth Avenue
New York, NY 10018
United States
Tel: +1 212 626 4337
Fax: +1 212 310 1696
william.devaney@bakermckenzie.com

© Law Business Research 2021

815 Connecticut Avenue, NW
Washington, DC 20006
United States
Tel: +1 202 452 7000
Fax: +1 202 452 7074
aleesha.fowler@bakermckenzie.com

www.bakermckenzie.com

BCL Solicitors LLP

51 Lincoln's Inn Fields
London, WC2A 3LZ
United Kingdom
Tel: +44 20 7430 2277
Fax: +44 20 7430 1101
rsallybanks@bcl.com
awarlow@bcl.com
aswan@bcl.com
www.bcl.com

BDO USA, LLP

100 Park Avenue
New York, NY 10017
United States
Tel: +1 212 885 8000
gpomerantz@bdo.com
dburget@bdo.com
www.bdo.com

Booking.com

Herengracht 597
Amsterdam, 1017 CE
Netherlands
Tel: +31 6 1557 1441
femi.thomas@booking.com
www.booking.com

Brown Rudnick LLP

8 Clifford Street
London, W1S 2LQ
United Kingdom
Tel: +44 20 7851 6000
Fax: +44 20 7851 6100
aamole@brownrudnick.com
aosullivan@brownrudnick.com
fcassidy-taylor@brownrudnick.com
www.brownrudnick.com

Cadwalader, Wickersham & Taft LLP

100 Bishopsgate
London, EC2N 4AG
United Kingdom
Tel: +44 20 7170 8700
kevin.roberts@cwt.com
duncan.grieve@cwt.com
charlotte.glaser@cwt.com

200 Liberty Street
New York, NY 10281
United States
Tel: +1 212 504 6000
Fax: +1 212 504 6666
anne.tompkins@cwt.com
robert.duncan@cwt.com
todd.blanche@cwt.com

700 Sixth Street, NW
Washington, DC 20001
United States
Tel: +1 202 862 2456
jodi.avergun@cwt.com
Tel: +1 202 862 2476
cheryl.risell@cwt.com
Fax: +1 202 862 2400

www.cadwalader.com

© Law Business Research 2021

Clifford Chance

Clifford Chance LLP
10 Upper Bank Street
Canary Wharf
London, E14 5JJ
United Kingdom
Tel: +44 20 7006 1000
Fax: +44 20 7006 5555
emily.goddard@cliffordchance.com
anna.kirkpatrick@cliffordchance.com
ellen.lake@cliffordchance.com
luke.tolaini@cliffordchance.com

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
benjamin.berringer@cliffordchance.com
meredith.george@cliffordchance.com
celeste.koeleveld@cliffordchance.com
christopher.morvillo@cliffordchance.com
daniel.silver@cliffordchance.com

www.cliffordchance.com

Cloth Fair Chambers

39-40 Cloth Fair
London, EC1A 7NT
United Kingdom
Tel: +44 20 7710 6444
aaronwatkins@clothfairchambers.com
alisonpople@clothfairchambers.com
nicholas.purnell@clothfairchambers.com
www.clothfairchambers.com

Cooley (UK) LLP

22 Bishopsgate
London, EC2N 4BQ
United Kingdom
Tel: +44 20 7583 4055
tepps@cooley.com
mkavanagh@cooley.com
alove@cooley.com
jmaskell@cooley.com
bsharrock@cooley.com
www.cooley.com

Corker Binning

The Cursitor Building
38 Chancery Lane
London, WC2A 1EN
United Kingdom
Tel: +44 20 7353 6000
Fax: +44 20 7353 6008
jp@corkerbinning.com
as@corkerbinning.com
www.corkerbinning.com

Cravath, Swaine & Moore LLP

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
United States
Tel: +1 212 474 1000
Fax: +1 212 474 3700
jburetta@cravath.com
mlew@cravath.com
jzhai@cravath.com
www.cravath.com

© Law Business Research 2021

Debevoise & Plimpton LLP

919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
beyannett@debevoise.com
dsarratt@debevoise.com
www.debevoise.com

DLA Piper LLP

1251 Avenue of the Americas
New York, NY 10020-1104
United States
Tel: +1 212 335 4500
Fax: +1 212 335 4501
john.hillebrecht@dlapiper.com
lisa.tenorio@dlapiper.com
eric.christofferson@dlapiper.com
www.dlapiper.com

Fountain Court Chambers

Fountain Court
Temple
London, EC4Y 9DH
United Kingdom
Tel: +44 20 7583 3335
Fax: +44 20 7353 0329
eld@fountaincourt.co.uk
rb@fountaincourt.co.uk
nxl@fountaincourt.co.uk
to@fountaincourt.co.uk
rjl@fountaincourt.co.uk
ser@fountaincourt.co.uk
www.fountaincourt.co.uk

Fox Williams LLP

10 Finsbury Square
London, EC2A 1AF
United Kingdom
Tel: +44 20 7628 2000
Fax: +44 20 7628 2100
jcarlton@foxwilliams.com
sganatra@foxwilliams.com
dmurphy@foxwilliams.com
www.foxwilliams.com

Freshfields Bruckhaus Deringer LLP

100 Bishopsgate
London, EC2P 2SR
United Kingdom
Tel: +44 20 7936 4000
Fax: +44 20 7832 7001
matthew.bruce@freshfields.com
ben.morgan@freshfields.com
alison.kirby-harris@freshfields.com
ali.sallaway@freshfields.com
www.freshfields.com

Goodwin

The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
United States
Tel: +1 212 813 8800
Fax: +1 212 355 3333
rstrassberg@goodwinlaw.com
mspillane@goodwinlaw.com
www.goodwinlaw.com

© Law Business Research 2021

Herbert Smith Freehills LLP

Exchange House
Primrose Street
London, EC2A 2EG
United Kingdom
Tel: +44 20 7374 8000
Fax: +44 20 7374 0888
brian.spiro@hsf.com
jessica.chappatte@hsf.com
www.herbertsmithfreehills.com

Jenner & Block LLP

Jenner & Block London LLP
25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Tel: +44 330 060 5400
Fax: +44 330 060 5499
aazarian@jenner.com

353 N Clark Street
Chicago, IL 60654-3456
United States
Tel: +1 312 222 9350
criely@jenner.com
gsignorelli@jenner.com

919 Third Avenue
New York, NY 10022-3908
United States
Tel: +1 212 891 1600
abarkow@jenner.com

www.jenner.com

Jones Day

250 Vesey Street
New York, NY 10281-1047
United States
Tel: +1 212 326 3939
Fax: +1 212 755 7306
jloonam@jonesday.com
randreoli@jonesday.com
www.jonesday.com

Kingsley Napley LLP

20 Bonhill Street
London, EC2A 4DN
United Kingdom
Tel: +44 20 7814 1200
Fax: +44 20 7490 2288
cday@kingsleynapley.co.uk
lhodges@kingsleynapley.co.uk
www.kingsleynapley.co.uk

Latham & Watkins

99 Bishopsgate
London, EC2M 3XF
United Kingdom
Tel: +44 20 7710 1000
stuart.alford.qc@lw.com
gail.crawford@lw.com
hayley.pizzey@lw.com
mair.williams@lw.com

1271 Avenue of the Americas
New York, NY 10020
United States
Tel: +1 212 906 1200
serrin.turner@lw.com
matthew.valenti@lw.com

www.lw.com

Linklaters LLP

One Silk Street
London, EC2Y 8HQ
United Kingdom
Tel: +44 20 7456 2000
Fax: +44 20 7456 2222
alison.wilson@linklaters.com
sinead.casey@linklaters.com
elly.proudlock@linklaters.com
nicholas.marshall@linklaters.com
www.linklaters.com

© Law Business Research 2021

McGuireWoods

5 New Street Square
London, EC4A 3BF
United Kingdom
Tel: +44 20 7632 1600
ftitus@mcguirewoods.com
mdossa@mcguirewoods.com
wboddy@mcguirewoods.com

77 West Wacker Drive, Suite 4100
Chicago, IL 60601-1818
United States
Tel: +1 312 849 8100
rheaton@mcguirewoods.com

888 16th Street NW, Suite 500
Black Lives Matter Plaza
Washington, DC 20006
United States
Tel: +1 202 857 1700
athornton-dibb@mcguirewoods.com

www. mcguirewoods.com

Mayer Brown

350 South Grand Avenue, 25th Floor
Los Angeles, CA 90071-1503
United States
Tel: +1 213 229 9500
gvanzura@mayerbrown.com

1221 Avenue of the Americas
New York, NY 10020-1001
United States
Tel: +1 212 506 2500
dstein@mayerbrown.com
bacohen@mayerbrown.com

1999 K Street, NW
Washington, DC 20006-1101
United States
Tel: +1 202 263 3000
jlinder@mayerbrown.com

www.mayerbrown.com

Mishcon de Reya LLP

Africa House
70 Kingsway
London, WC2B 6AH
United Kingdom
Tel: +44 20 3321 7000
Fax: +44 20 7404 5982
ben.brandon@mishcon.com
johanna.walsh@mishcon.com
mellissa.curzon-berners@mishcon.com
www.mishcon.com

Nokia Corporation

3 Sheldon Square
Paddington
London, W2 6PR
United Kingdom
Tel: +44 7949 451 112
daniel.igra@nokia.com
www.nokia.com

Norton Rose Fulbright

Norton Rose Fulbright LLP
3 More London Riverside
London, SE1 2AQ
United Kingdom
Tel: +44 20 7283 6000
pamela.reddy@nortonrosefulbright.com
katie.stephen@nortonrosefulbright.com
andrew.reeves@nortonrosefulbright.com

Norton Rose Fulbright US LLP
799 9th Street NW, Suite 1000
Washington, DC 20001
United States
Tel: +1 202 662 0200
kevin.harnisch@nortonrosefulbright.com
ilana.sinkin@nortonrosefulbright.com

www.nortonrosefulbright.com

© Law Business Research 2021

Outer Temple Chambers

The Outer Temple
222 Strand
London, WC2R 1BA
United Kingdom
Tel: +44 20 7353 6381
Fax: +44 870 220 3256
michael.bowesqc@outertemple.com
www.outertemple.com

Ropes & Gray LLP

60 Ludgate Hill
London, EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
matthew.burn@ropesgray.com
sarah.lambert-porter@ropesgray.com
amanda.raad@ropesgray.com
judith.seddon@ropesgray.com
sean.seelinger@ropesgray.com
zaneta.wykowska@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
United States
Tel: +1 617 951 7000
Fax: +1 617 951 7050
patrick.roath@ropesgray.com

191 North Wacker Drive, 32nd Floor
Chicago, IL 60606
United States
Tel: +1 312 845 1200
Fax: +1 312 845 5500
jaime.feeney@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036-8704
United States
Tel: +1 212 596 9600
Fax: +1 212 596 9090
lisa.bebchick@ropesgray.com
meghan.gilliganpalermo@ropesgray.com
chloe.gordils@ropesgray.com
david.hennes@ropesgray.com
abraham.lee@ropesgray.com
michael.mcgovern@ropesgray.com
alexander.simkin@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
ama.adams@ropesgray.com
jeel.oza@ropesgray.com

www.ropesgray.com

Skadden, Arps, Slate, Meagher & Flom (UK) LLP

40 Bank Street
Canary Wharf
London, E14 5DS
United Kingdom
Tel: +44 20 7519 7000
Fax: +44 20 7519 7070
elizabeth.robertson@skadden.com
vanessa.mcgoldrick@skadden.com
jason.williamson@skadden.com
www.skadden.com

© Law Business Research 2021

Slaughter and May

One Bunhill Row
London, EC1Y 8YY
United Kingdom
Tel: +44 20 7600 1200
Fax: +44 20 7090 5000
jonathan.cotton@slaughterandmay.com
holly.ware@slaughterandmay.com
ella.williams@slaughterandmay.com
www.slaughterandmay.com

Sullivan & Cromwell LLP

125 Broad Street
New York, NY 10004-2498
United States
Tel: +1 212 558 4000
Fax: +1 212 558 3588
bourtinn@sullcrom.com
www.sullcrom.com

Walden Macht & Haran LLP

250 Vesey Street, 27th Floor
New York, NY 10281
United States
Tel: +1 212 335 2030
Fax: +1 212 335 2040
mwilliams@wmhlaw.com
apatel@wmhlaw.com
jgardener@wmhlaw.com
www.wmhlaw.com

Willkie Farr & Gallagher LLP

Citypoint
1 Ropemaker Street
London, EC2Y 9AW
United Kingdom
Tel: +44 20 3580 4700
rmitchell@willkie.com
sosborn-king@willkie.com
yyuen@willkie.com

1875 K Street, NW
Washington, DC 20006-1238
United States
Tel: +1 202 303 1000
Fax: +1 202 303 2000
dmortlock@willkie.com
ncronin@willkie.com
bmosman@willkie.com
ael-gamal@willkie.com

www.willkie.com

© Law Business Research 2021

Index to Volume I

All references are to section numbers

Accounting issues
see **Forensic accounting**
Admissions
UK, 23.3.2
US, 24.5.4
Antitrust laws
antitrust leniency programme, 10.1.2.2
extraterritoriality, 29.7
Arbitration
class actions, 35.3.1.5
parallel civil proceedings, 34.6.5
stay of proceedings, 34.2.2
Asset recovery (UK)
civil recovery orders, 25.8
confiscation orders, 25.3
cross-border investigations
account monitoring orders, 17.3.2
confiscation orders, 17.3.3
forfeiture orders, 17.3.3
freezing orders, 17.3.1
restraint orders, 17.3.1
restitution orders, 25.14
restraint orders, 25.9
Asset recovery (US)
civil and criminal asset forfeiture, 31.2.5.2
cross-border investigations, 18.6
pretrial asset freeze orders, 31.2.5.1
Attorney–client privilege
see **Privilege (US)**

Bases of corporate liability
introduction, 1.1
UK, 1.1.1
US, 1.1.2
Beginning internal investigations (UK)
decision to begin investigation, 5.3
document management
collection, 5.6.2
documents in other jurisdictions, 5.6.4
importance of record-keeping, 5.6.5
introduction, 5.6
preservation, 5.6.1
review, 5.6.3
introduction, 5.1
notifying relevant authorities, 5.2
oversight and management of investigation, 5.4
scoping the investigation, 5.5
timing, 5.3
Beginning internal investigations (US)
assessing necessity of investigation, 6.2
control of investigation, 6.4

© Law Business Research 2021

determining scope of investigation
developing a work plan, 6.5.3
identifying necessary partners, 6.5.2
introduction, 6.5
key documents and scoping interviews, 6.5.1
document management
collection, 6.6.2
documents in other jurisdictions, 6.7
preservation, 6.6.1
review, 6.6.3
identifying client, 6.3
in-house or external counsel, 6.4
introduction, 6.1
Bribery
UK
compliance, 46.2.1, 46.4.1.1
extraterritoriality, 28.2
'tainted' contracts, 34.6.1
whistleblowing, 19.3.2.1
US
extraterritoriality, 29.8
generally, 26.7.1
Business Banking Resolution Service complaints
parallel civil proceedings, 34.3.5

Cautions
UK, 7.9, 15.4.1
Upjohn warnings, 8.3, 37.3.1
Civil recovery orders
corporate penalties, 25.8
global settlements, 23.2.1.1
Class actions
UK
collective redress schemes, 34.3.7
competition law claims, 34.3.6
FOS/BBRS complaints, 34.3.5
group litigation orders, 34.3.2
introduction, 34.3
joint claims, 34.3.3
representative actions, 34.3.1
test cases, 34.3.4
US
arbitration agreements, 35.3.1.5
opt-outs, 35.3.1.6
overview, 35.3.1.1
procedure, 35.3.1.3
public records as basis for filing, 35.3.1.2
standards, 35.3.1.3
statutory reforms, 35.3.1.4
Collective redress schemes
parallel civil proceedings, 34.3.7
Common interest privilege
UK, 36.5
US, 37.1.3
Compensation
UK
corporate penalties, 25.2
individual penalties, 30.1.5
US, 31.2.6
Competition and Markets Authority
whistleblowing, 19.2.5
Competition law
antitrust laws
antitrust leniency programme, 10.1.2.2
extraterritoriality, 29.7
parallel civil proceedings, 34.3.6
Complaints
customer and competitor complaints, 2.2.2.5
internal complaints, 2.2.1.1
investor complaints, 2.2.2.4
Compliance
compliance programmes, 1.3.4
conclusion, 46.8
considerations from previous resolutions, 46.7
criminal liability (UK)
Bribery Act 2010, 46.2.1
Criminal Finances Act 2017, 46.2.2
distinctions between failure-to-prevent offences, 46.2.3
Money Laundering Regulations 2017, 46.2.4
culture and effective compliance, 46.5

© Law Business Research 2021

deferred prosecution agreements, 46.6
financial penalties, 46.6
guidance (UK)
Bribery Act 2010, 46.4.1.1
FCA Financial Crime Guide, 46.4.1.3
HMRC Facilitation of Tax Evasion Guidance, 46.4.1.2
introduction, 46.4
Joint Money Laundering Steering Group guidance, 46.4.1.4
SFO Guidance on Evaluating a Compliance Programme, 46.4.1.5
guidance (US)
DOJ FCPA Opinion Procedure, 46.4.2.4
DOJ Guidance on Evaluation of Corporate Compliance Systems, 46.4.2.2
DOJ Guidance on Evaluation of Corporate Compliance Systems in Criminal Antitrust Investigations, 46.4.2.3
SEC/DOJ Resource Guide, 46.4.2.1
introduction, 1.3.4, 46.1
prosecutorial decision-making, 46.6
regulatory liability (UK)
FCA Principles, 46.3.1
other regulators, 46.3.2
risk management, 2.5

Concurrent settlements
UK, 34.9
US, 35.5.2

Confidential information
need for confidentiality, 36.2.1

Confiscation
UK
corporate penalties, 25.3
cross-border investigations, 17.3.3
individual penalties, 30.1.4
US, 31.2.5

Conspiracy
conspiracy to commit offences abroad, 28.6.2
conspiracy to defraud, 28.6.1
inchoate offences, 28.6.3
introduction, 28.6

Co-operation credit
UK
continuing co-operation, 3.6.1.2
generally, 3.6.1
timing of self-reporting, 3.6.1.1
waiver of privilege, 3.6.1.3
US
Benczkowski Memorandum, 4.3.1.1
Corporate Enforcement Policy, 4.3.1.1
DOJ co-operation credit, 4.3.1.1
introduction, 4.3.1
SEC co-operation credit, 4.3.1.2
waiver of privilege, 37.4.1

Co-operation with authorities (UK)
compliance, 9.5
conclusion, 9.10
decision to co-operate, 9.1
initial considerations, 9.2
introduction, 9.1
meaning of co-operation
conducting approved internal investigation, 9.3.4
data handling, 9.3.5
definition and descriptions, 9.3.1
facilitating access to witnesses, 9.3.6
genuine and continual co-operation, 9.3.2
highlighting exculpatory material, 9.3.8
privilege, 9.3.7
prompt self-reporting to authorities, 9.3.3
multi-agency and cross-border investigations
generally, 9.8
strategies for dealing with multiple authorities, 9.9
new management, 9.6
penalty mitigation, 9.4

© Law Business Research 2021

reasons for co-operation, 9.7
status of corporate, 9.2
Co-operation with authorities (US)
case studies, 10.1.4
CFTC approach, 10.1.3
DOJ general approach, 10.1.1
DOJ policies
antitrust leniency programme, 10.1.2.2
False Claims Act, 10.1.2.3
FCPA Pilot Program and Civil Enforcement Policy, 10.1.2.1
introduction, 10.1.2
key benefits and drawbacks
disruption to business, 10.2.4
excessive co-operation between counsel and government, 10.2.6
exposure to civil litigation, 10.2.5
financial cost, 10.2.3
introduction, 10.2
penalty mitigation or avoidance, 10.2.1
suspension and debarment, 10.2.2
meaning of co-operation, 10.1
multi-agency and cross-border investigations
cross-border coordination, 10.3.2
DOJ policy against 'piling on', 10.3.3
multi-agency coordination, 10.3.1
other federal agencies' approaches, 10.1.3
other options besides co-operation, 10.2.7
SEC approach, 10.1.3
Corporate criminal liability
bases of liability, 1.1
UK, 1.1.1
US, 1.1.2
Corporate governance
see **Directors' duties (UK)**; **Directors' duties (US)**; **Environmental, social and governance investigations**
Corporate penalties (UK)
see also **Individual penalties (UK)**
approved persons, 25.13
civil recovery orders, 25.8
compensation orders, 25.2
confiscation orders, 25.3
costs, 25.6
criminal financial penalties, 25.1
debarment, 25.15
director disqualification, 25.7
fines, 25.4
guilty pleas, 25.5
outcomes under DPA, 25.16
regulatory financial penalties, 25.11
restitution orders, 25.14
restraint orders, 25.9
serious crime prevention orders, 25.10
withdrawal of authorisation, 25.12
Corporate penalties (US)
see also **Individual penalties (US)**
civil penalties, 26.3
conclusion, 26.8
disgorgement and prejudgment interest, 26.4
injunctions, 26.5
introduction, 26.1
maximum financial penalties, 26.2.1
other consequences, 26.6
sentencing guidelines, 26.2.2
specific statutes
export controls and trade sanctions, 26.7.3
federal criminal money laundering, 26.7.2
Foreign Corrupt Practices Act, 26.7.1
introduction, 26.7
RICO, 26.7.4
Costs
corporate penalties, 25.6
individual penalties, 30.1.7
Criminal Finances Act 2017
compliance, 46.2.2
extraterritoriality, 28.4
whistleblowing, 19.3.2.2
Cross-border investigations (UK)
asset recovery
account monitoring orders, 17.3.2

© Law Business Research 2021

confiscation orders, 17.3.3
forfeiture orders, 17.3.3
freezing orders, 17.3.1
restraint orders, 17.3.1
co-operation with authorities
generally, 9.8, 17.2
strategies for dealing with multiple authorities, 9.9
extradition
bars to extradition, 17.4.4
category 1 territories, 17.4.1
category 2 territories, 17.4.2
European arrest warrants, 17.4.1
forum, 17.4.4.3
human rights, 17.4.4.1
introduction, 17.4
other territories, 17.4.3
proportionality, 17.4.4.2
interviews, 17.3.4
introduction, 17.1
production of documents, 17.3.6
reputation, 17.6
search and seizure, 17.3.5
settlement, 17.5
Cross-border investigations (US)
arrest and bail, 18.2.1
assessing client's status, 18.4.1
asset recovery, 18.6
client-centred lawyering, 18.8
collateral consequences, 18.7
confidentiality, 18.2.2
co-operation with authorities
decision to co-operate, 18.4.2
DOJ policy against 'piling on', 10.3.3
generally, 10.3.2
counsel selection, 18.4.4
decision to co-operate
criminal or civil proceedings, 18.4.2.1
internal investigations, 18.4.2.2
evidence
foreign restrictions on information transfer, 18.5.2
internal investigations, 18.5.3
preservation, 18.2.2
privilege, 18.5.1
extradition
appeals, 18.3.5
applicable law, 18.3.1
decision to litigate or waive extradition, 18.3.3
defences, 18.3.4
introduction, 18.3
procedure, 18.3.2
recent developments, 18.3.6
initial conversations with client, 18.2.3
introduction, 18.1
multiple authorities
evidence obtained pursuant to MLAT, 18.4.3.2
voluntary interviews, 18.4.3.1
preliminary considerations, 18.2
privilege, 18.5.1
settlement, 18.4.5
strategic considerations, 18.4
voluntary interviews, 18.4.3.1
Cryptocurrencies
forensic accounting, 22.12
Cybersecurity
cybercrime, 41.1.1
enforcement (UK)
ICO's powers, 41.5.1
introduction, 41.5
reporting breaches, 41.5.2
enforcement (US)
introduction, 41.5.3
reporting breaches, 41.5.4
introduction, 41.1
investigating cyber breaches, 41.4
legal framework (UK)
introduction, 41.2.1
laws criminalising cyberattacks, 41.2.1.1
positive obligations for victims, 41.2.1.2
legal framework (US)
federal law, 41.2.2.1
introduction, 41.2.2
state law, 41.2.2.2
motivations of cybercriminals, 41.1.2

© Law Business Research 2021

proactive cybersecurity, 41.3
recent cyberattacks, 41.1.3

Dark web
forensic accounting, 22.12
Data
see also **Data protection**
analysis of financial data, 22.7
analysis of non-financial records, 22.8
conclusion, 22.13
cryptocurrencies, 22.12
e-discovery and litigation holds, 22.4
forensic data science and analytics
corroborating allegations, 22.6.2
data mining to detect fraud or non-compliance, 22.6.1
generally, 22.6
use in investigations, 22.6.3
introduction, 22.1
preservation, mitigation and stabilisation, 22.3
regulator expectations, 22.2
review of supporting documents and records, 22.10
tracing assets and other methods of recovery, 22.11
use of external data in investigations, 22.9
violation of internal controls, 22.5
Data protection
data security breaches
parallel civil proceedings, 34.6.7
self-reporting, 3.4.2
internal investigations (UK)
consent for processing, 40.2.3
criminal offences data, 40.2.5
cross-border data transfer, 40.2.7
data minimisation, 40.2.2
employee monitoring, 40.2.9
introduction, 40.2
legitimate interest, 40.2.4
public interest, 40.2.6
special category data, 40.2.5
third parties, 40.2.8
transparency, 40.2.1
internal investigations (US), 40.3
introduction, 40.1
investigations by authorities (UK)
generally, 40.4
providing data to authorities, 40.4.1
investigations by authorities (US), 40.5
practical considerations, 40.7
publicity, 38.5.4
whistleblowers
introduction, 40.6
right to access data, 40.6.2
whistleblowing policies, 40.6.1
Defamation proceedings
parallel civil proceedings, 34.6.4
Deferred prosecution agreements
see also **Global settlements (UK)**; **Global settlements (US)**
compliance, 1.3.4, 46.6
UK
corporate criminal liability, 1.1.1
culture, 3.2
evolution of link with self-reporting, 3.3
generally, 23.2.1.2, 23.4, 25.16
individuals, 30.1
introduction, 3.1
reporting obligations, 3.4.3
timing, 3.6.1.1
whistleblowing, 3.2
US
civil proceedings, 24.4.2
criminal proceedings, 24.4.1
Derivative claims
UK
generally, 34.4.1
practical considerations, 34.4.3
risk management, 2.2.2.4
US
indemnification and advancement, 35.3.2.3
overview, 35.3.2.1
procedure, 35.3.2.2
standards, 35.3.2.2

© Law Business Research 2021

Directors' duties (UK)
accepting benefits from third parties, 42.2.1.6
acting within powers, 42.2.1.1
Companies Act 2006, 42.2.1
conclusion, 42.4
conflicts of interest, 42.2.1.5
Corporate Governance Code, 42.2.2
declaration of interests in proposed transactions, 42.2.1.7
expectations versus obligations, 42.3
FRC Guidance on Board Effectiveness, 42.2.5
independent judgment, 42.2.1.3
introduction, 42.1
other duties, 42.2.1.8
promoting success of company, 42.2.1.2
QCA Corporate Governance Code, 42.2.3
reasonable care, skill and diligence, 42.2.1.4
reporting on s.172 compliance, 42.2.6
Senior Manager Conduct Rules, 42.2.7
sources of duties, 42.2
Wates Corporate Governance Principles, 42.2.4
Directors' duties (US)
duty of care, 43.2.1
fiduciary duties, 43.2
introduction, 43.1
liability for breach of duty
business judgment rule, 43.3.2
Caremark claims in private civil actions, 43.3.1
loyalty, 43.2.2
oversight in investigations, 43.6
oversight under securities laws, 43.2.3
regulatory enforcement actions, 43.4
SEC Whistleblower Program, 43.5
strategic considerations, 43.7
Disclosure
see **Production of documents/information**; **Self-reporting to authorities (UK)**; **Self-reporting to authorities (US)**
Disgorgement
corporate penalties, 26.4
Disqualification
UK, 25.7, 30.1.6
US, 31.2.7
Document management
see also **Production of documents/information**
UK
document collection, 5.6.2
document preservation, 5.6.1
document review, 5.6.3
documents in other jurisdictions, 5.6.4
importance of record-keeping, 5.6.5
introduction, 5.6
US
document collection, 6.6.2
document preservation, 6.6.1
document review, 6.6.3
documents in other jurisdictions, 6.7
Dodd-Frank Act
whistleblowing, 20.1.1
Double jeopardy
conclusion, 1.2.6
EU law, 1.2.3
European human rights jurisprudence
CJEU, 1.2.4.2
ECtHR, 1.2.4.1
France, 1.2.5
introduction, 1.2
UK, 1.2.1
US, 1.2.2
Due diligence
risk management, 2.2.1.3

Electronic documents/data
see **Data**
Employee rights (UK)
employment law, 13.1.2
indemnification and insurance

© Law Business Research 2021

advocating for indemnification when not otherwise clear, 13.3.2
cap on insurance policy, 13.3.4.1
company commitment to continue indemnification, 13.3.4.2
company policies, by-laws or local laws, 13.3.1.1
determining whether individual is indemnified, 13.3.1
directors' and officers' insurance, 13.3.1.2
employment contract, 13.3.1.1
ensuring sufficient funds for protracted investigation, 13.3.4
failure to co-operate with investigation, 13.3.3.2
insurance policies of employer, 13.3.1.2
situations where indemnification may cease, 13.3.3
violation of undertaking to company, 13.3.3.1
joint defence agreements
individuals and company, 13.2.2.1
individuals and their counsel, 13.2.2.2
monitoring of electronic communications, 40.2.9
privilege
communications using employer email, 13.4.2
communications with colleagues or people involved in underlying events, 13.4.1.1
communications with company counsel, 13.4.1.2
representation
interviewing client, 13.2.1.1
joint defence agreements, 13.2.2
requesting documents and information, 13.2.1.2
statutory rights, 13.1
suspension
generally, 13.1.1.1
reasonable grounds, 13.1.1.2
remuneration, 13.1.1.3
Employee rights (US)
covid-19, 14.5
freedom from retaliation, 14.2
indemnification
advocating for indemnification, 14.6.3
cessation of indemnification, 14.7
company policies, 14.6.2.3
corporate by-laws, 14.6.2.1
determining whether individual is indemnified, 14.6.1
employment contracts, 14.6.2.3
failure to co-operate with investigation, 14.7
insurance policies of employer, 14.6.2.4
introduction, 14.6
local law in state of incorporation, 14.6.2.2
potential sources of indemnification, 14.6.2
introduction, 14.1
privacy
workplace searches, 14.4.1
workplace surveillance, 14.4.2
privilege, 14.8
representation
interviews without employee's counsel, 14.3.1
right to representation, 14.3
separate representation arranged by employer, 14.3.2
Employment law
UK, 34.6.6
US, 35.3.3.4
Encouraging or assisting crime
extraterritoriality, 28.6.3
Environmental, social and governance investigations
corporate standards, 47.3.3
environmental issues, 47.2
financial risk, 47.4.5
governance issues, 47.2
greenwashing, 47.2

© Law Business Research 2021

heightened business risk, 47.4.5
introduction, 47.1
investigator expertise and independence, 47.4.2
legal and regulatory frameworks
corporate standards, 47.3.3
generally, 47.3
hard law, 47.3.1
soft law, 47.3.2
legal risk, 47.4.5
operational risk, 47.4.5
particularities, 47.4
privilege, 47.4.3
remediation, 47.4.6
reporting, 47.4.3
reputational risk, 47.4.5
risk management, 2.4
social issues, 47.2
stakeholder engagement, 47.4.4
standards and principles
corporate standards, 47.3.3
generally, 47.3.2
international standards and principles, 47.3.2.1
voluntary standards and principles, 47.3.2.2
transparency, 47.4.3
triggers for investigations, 47.2, 47.4.1
UN Guiding Principles on Business and Human Rights, 47.3.2.1

European arrest warrants
extradition, 17.4.1

Evidence
cross-border investigations (US)
foreign restrictions on information transfer, 18.5.2
internal investigations, 18.5.3
preservation, 18.2.2
privilege, 18.5.1
parallel civil proceedings (UK)
collateral use of disclosed documents, 34.7.3
reliance by authority on court findings, 34.7.2
reliance by court on authorities' findings, 34.7.1
parallel civil proceedings (US)
collateral use of disclosed documents, 35.4.3
introduction, 35.4
privilege waivers and disclosure obligations, 35.4.4
reliance by civil litigants on regulatory findings, 35.4.1
reliance by regulators on court findings, 35.4.2

Extradition
bases for extradition, 32.2
contemporary issues
Brexit, 32.5.3
Interpol red notices, 32.5.2
US extraditions, 32.5.1
core concepts, 32.3
cross-border investigations (UK)
bars to extradition, 17.4.4
category 1 territories, 17.4.1
category 2 territories, 17.4.2
European arrest warrants, 17.4.1
forum, 17.4.4.3
human rights, 17.4.4.1
introduction, 17.4
other territories, 17.4.3
proportionality, 17.4.4.2
cross-border investigations (US)
appeals, 18.3.5
applicable law, 18.3.1
decision to litigate or waive extradition, 18.3.3
defences, 18.3.4
introduction, 18.3
procedure, 18.3.2
recent developments, 18.3.6
double (dual) criminality, 32.3.1
double jeopardy, 32.3.4
human rights, 32.3.5
introduction, 32.1
ne bis in idem, 32.3.4
political motivation, 32.3.3
specialty, 32.3.2

© Law Business Research 2021

trends
decreasing requirement to prove *prima facie* case, 32.4.3
expedition, 32.4.4
growth of international co-operation, 32.4.1
'judicialisation' of extradition process, 32.4.2
Extraterritoriality (UK)
Bribery Act 2010
corporate offence under s.7, 28.2.2
introduction, 28.2
offences under ss.1, 2 and 6, 28.2.1
conspiracy
conspiracy to commit offences abroad, 28.6.2
conspiracy to defraud, 28.6.1
inchoate offences, 28.6.3
introduction, 28.6
Criminal Finances Act 2017, 28.4
encouraging or assisting crime, 28.6.3
financial sanctions, 28.5
mutual legal assistance, 28.7
overview, 28.1
Proceeds of Crime Act 2002
civil recovery orders, 28.3.2
money laundering offences, 28.3.1
tax evasion, 28.4
transparency of corporate ownership, 28.7
Extraterritoriality (US)
antitrust laws, 29.7
Commodity Exchange Act, 29.6
conclusion, 29.12
criminal versus civil cases, 29.3
extraterritorial reach of US laws, 29.1
Foreign Corrupt Practices Act, 29.8
money laundering, 29.10
power to obtain evidence located overseas, 29.11
RICO, 29.4
sanctions, 29.9
securities laws
introduction, 29.2
Morrison decision, 29.2.1
post-*Morrison* developments, 29.2.2
wire fraud, 29.5

False Claims Act
DOJ policies, 10.1.2.3
effects of filing *qui tam* action, 20.4.2
introduction, 20.4
procedure for *qui tam* actions, 20.4.1
Fifth Amendment
double jeopardy, 1.2.2
witness interviews, 16.5
Financial Conduct Authority
production of documents/information
compulsory requests, 11.2.3.1
FCA obligations, 11.2.3.3
voluntary production, 11.2.3.2
Rules
approved persons, 19.3.1.3
Individual Conduct Rules, 19.3.1.1
introduction, 19.3.1
Senior Manager Conduct Rules, 19.3.1.2
self-reporting, 3.4.4
systems and controls requirements
internal whistleblowing arrangements, 19.2.4.1
introduction, 19.2.4
settlement agreements with workers, 19.2.4.3
whistleblowers' champion, 19.2.4.2
Financial Ombudsman Service complaints
parallel civil proceedings, 34.3.5
Financial sanctions breaches
self-reporting, 3.4.2
Fines
corporate penalties
UK, 25.4
US, 26.2
individual penalties
UK, 30.1.2
US, 31.2.3
Foreign Corrupt Practices Act
extraterritoriality, 29.8
FCPA Pilot Program, 10.1.2.1

© Law Business Research 2021

penalties, 26.7.1
Forensic accounting
analysis of financial data, 22.7
analysis of non-financial records, 22.8
conclusion, 22.13
cryptocurrencies, 22.12
dark web, 22.9
e-discovery and litigation holds, 22.4
forensic data science and analytics
corroborating allegations, 22.6.2
data mining to detect fraud or non-compliance, 22.6.1
generally, 22.6
use in investigations, 22.6.3
introduction, 22.1
preservation, mitigation and stabilisation, 22.3
private records, 22.9
publicly available information, 22.9
regulator expectations, 22.2
review of supporting documents and records, 22.10
tracing assets and other methods of recovery, 22.11
use of external data in investigations, 22.9
violation of internal controls, 22.5
Forfeiture
see **Asset recovery (UK)**; **Asset recovery (US)**

GDPR
see **Data protection**
Global settlements (UK)
ability to secure global settlement, 23.2.2.2
admissions, 23.3.2
civil recovery orders, 23.2.1.1
cross-border investigations, 17.5
deferred prosecution agreements, 23.2.1.2, 23.4
in-house considerations
conclusion, 27.7
customers, 27.5
employees, 27.4
introduction, 27.1
other stakeholders, 27.6
regulators and enforcement agencies, 27.6
senior management, 27.2
shareholders, 27.3
initial considerations, 23.2
introduction, 23.1
legal considerations, 23.3
legal professional privilege, 23.3.1
negotiated plea agreements, 23.2.1.3
options for seeking settlement, 23.2.1
oral presentations to prosecuting authorities, 23.2.4
practical issues, 23.4
resolving parallel investigations
foreign authorities, 23.5.2
introduction, 23.5
other domestic authorities, 23.5.1
strategic considerations, 23.2.2
timing of settlement, 23.2.2.1
written submissions to prosecuting authorities, 23.2.3
Global settlements (US)
admissions, 24.5.4
collateral consequences, 24.5.3
consent orders, 24.4.2
continuing obligations, 24.5.2
cross-border investigations, 18.4.5
deferred prosecution agreements
civil proceedings, 24.4.2
criminal proceedings, 24.4.1
follow-on civil litigation, 24.5.4
guilty pleas, 24.4.1
in-house considerations
conclusion, 27.7
customers, 27.5
employees, 27.4
introduction, 27.1
other stakeholders, 27.6
regulators and enforcement agencies, 27.6
senior management, 27.2
shareholders, 27.3
introduction, 24.1

© Law Business Research 2021

key settlement terms
admissions and follow-on civil litigation, 24.5.4
collateral consequences, 24.5.3
continuing obligations, 24.5.2
introduction, 24.5
monetary penalties, 24.5.1
legal considerations, 24.3
limitation periods, 24.3.2
monetary penalties, 24.5.1
non-prosecution agreements
civil proceedings, 24.4.2
criminal proceedings, 24.4.1
privilege, 24.3.1
prosecutorial settlements, 24.4.1
regulatory settlements, 24.4.2
resolving parallel investigations
foreign authorities, 24.6.2
other domestic authorities, 24.6.1
strategic considerations, 24.2
tolling agreements, 24.3.2

Governance
see **Directors' duties (UK)**; **Directors' duties (US)**; **Environmental, social and governance investigations**

Greenwashing
ESG investigations, 47.2

Group litigation orders
parallel civil proceedings, 34.3.2

Human rights
double jeopardy
CJEU, 1.2.4.2
ECtHR, 1.2.4.1
extradition, 17.4.4.1, 32.3.5
UN Guiding Principles on Business and Human Rights, 47.3.2.1
whistleblowing, 19.2.7

Imprisonment
UK, 30.1.1
US, 31.2.2

Indemnification and insurance for employees
see **Employee rights (UK)**; **Employee rights (US)**

Individual penalties (UK)
see also **Corporate penalties (UK)**
criminal liability
compensation orders, 30.1.5
confiscation orders, 30.1.4
costs, 30.1.7
disqualification orders, 30.1.6
fines, 30.1.2
imprisonment, 30.1.1
introduction, 30.1
unexplained wealth orders, 30.1.3
regulatory liability, 30.2
third-party rights, 30.3

Individual penalties (US)
see also **Corporate penalties (US)**
collateral consequences of conviction, 31.2.7
confiscation of assets
civil and criminal asset forfeiture, 31.2.5.2
pretrial asset freeze orders, 31.2.5.1
prosecutorial discretion
DOJ enforcement priorities and policies, 31.1.3
generally, 31.1.1
individual accountability for wrongdoing, 31.1.4
Principles of Federal Prosecution, 31.1.2
sentencing
collateral consequences of conviction, 31.2.7
compensation orders, 31.2.6
confiscation of assets, 31.2.5
fines, 31.2.3
generally, 31.2.1
imprisonment, 31.2.2
probation, 31.2.4

Information Commissioner's Office
production of documents/information, 11.2.4

© Law Business Research 2021

Injunctions
corporate penalties, 26.5
Internal audit function
risk management, 2.2.1.2
Internal investigations (UK)
see also **Employee rights (UK)**; **Witness interviews (UK)**
data protection
consent for processing, 40.2.3
criminal offences data, 40.2.5
cross-border data transfer, 40.2.7
data minimisation, 40.2.2
employee monitoring, 40.2.9
introduction, 40.2
legitimate interest, 40.2.4
public interest, 40.2.6
special category data, 40.2.5
third parties, 40.2.8
transparency, 40.2.1
document management
collection, 5.6.2
documents in other jurisdictions, 5.6.4
importance of record-keeping, 5.6.5
introduction, 5.6
preservation, 5.6.1
review, 5.6.3
introduction, 5.1
representation in interviews
advising employee whether to attend, 15.2.3
lawyer's role in interview, 15.2.4
lawyer's role prior to interview, 15.2.2
when employees need own lawyer, 15.2.1
scoping the investigation, 5.5
Internal investigations (US)
see also **Employee rights (US)**; **Witness interviews (US)**
assessing necessity of investigation, 6.2
control of investigation, 6.4
data protection, 40.3
determining scope of investigation
developing a work plan, 6.5.3
identifying necessary partners, 6.5.2
introduction, 6.5
key documents and scoping interviews, 6.5.1
document management
collection, 6.6.2
documents in other jurisdictions, 6.7
preservation, 6.6.1
review, 6.6.3
identifying client, 6.3
in-house or external counsel, 6.4
introduction, 6.1
representation in interviews
conclusion, 16.6
current or former employees, 16.2.1
decision to be interviewed, 16.3.1, 16.3.2
introduction, 16.1
joint defence agreements, 16.2.3
kinds and scope of representation, 16.2
pool counsel, 16.2.2
preparation, 16.4
procedure in government interviews, 16.5
Interviews
see **Representation in interviews (UK)**; **Representation in interviews (US)**; **Witness interviews (UK)**; **Witness interviews (US)**

Joint claims
parallel civil proceedings, 34.3.3
Joint defence agreements
UK, 13.2.2
US, 16.2.3

Legal advice/legal professional privilege
see **Privilege (UK)**
Legal representation
see **Representation in interviews (UK)**; **Representation in interviews (US)**

© Law Business Research 2021

Litigation privilege
see **Privilege (UK)**

Media
ESG investigations, 47.4.3
publicity (UK)
after commencement of investigation/prosecution, 38.3.2
determining remit of PR team, 38.2.2
identifying a PR team, 38.2.1
self-reporting, 38.2.4
tabletop exercises, 38.2.3
publicity (US)
juries, 39.2.2
media as investigative/evidential tool, 39.2.1
risks and rewards of publicity, 39.3
reporting restrictions (UK)
automatic restrictions, 38.5.2.2
deferred prosecution agreements, 38.5.2.3
discretionary restrictions, 38.5.2.3
generally, 38.5.2.1
preparatory hearings, 38.5.2.3
prosecution appeals, 38.5.2.3
public access to court documents/information, 38.5.3
strict liability rule, 38.5.2.3
reporting restrictions (US)
consulting PR experts, 39.1.6
covid-19 impact, 39.1.5
discovery of internal corporate communications, 39.1.4
introduction, 39.1.1
investigatory and pretrial stage, 39.1.2
trial and post-trial stage, 39.1.3
risk management, 2.2.2.2
Money laundering
extraterritoriality
UK, 28.3.1
US, 29.10
federal criminal money laundering, 26.7.2
self-reporting, 3.4.1
Monitorship
circumstances requiring a monitor, 33.3
conclusion, 33.7
costs and other considerations, 33.6
duration, 33.5.2
evolution of modern monitor
UK, 33.2.2
US, 33.2.1
interviewing witnesses, 33.5.4
introduction, 33.1
recommendations and reports, 33.5.5
reviewing documents, 33.5.4
role of monitor, 33.5
scope, 33.5.1
selection of monitor, 33.4
work plans, 33.5.3
Mutual legal assistance
extraterritoriality, 28.7
multi-agency and cross-border investigations, 9.8, 9.9
production of documents/information (UK)
Brexit, 11.5.3
information outside UK, 11.5.2
introduction, 11.5.1
requests into UK, 11.5.4
production of documents/information (US), 11.5.5

Negotiated plea agreements
global settlements, 23.2.1.3
Negotiating global settlements
see **Global settlements (UK); Global settlements (US)**
Non-disclosure agreements
whistleblowing, 19.2.3, 19.4.4.2

Open justice
derogations, 38.5.1.2
generally, 38.5.1.1
remote hearings, 38.6
Opinion Procedure
compliance, 46.4.2.4

© Law Business Research 2021

Overseas employee interviews
UK, 7.14
US, 8.2

Parallel civil proceedings (UK)
arbitration, 34.6.5
Business Banking Resolution Service complaints, 34.3.5
civil law bribery, 34.6.1
collective redress schemes, 34.3.7
competition law claims, 34.3.6
conclusion, 34.10
concurrent settlements, 34.9
contractual provisions, 34.6.2
coordination with internal investigations team, 34.8.1
data security breaches, 34.6.7
defamation proceedings, 34.6.4
derivative claims
generally, 34.4.1
practical considerations, 34.4.3
employment law, 34.6.6
evidence
collateral use of disclosed documents, 34.7.3
reliance by authority on court findings, 34.7.2
reliance by court on authorities' findings, 34.7.1
Financial Ombudsman Service complaints, 34.3.5
group litigation orders, 34.3.2
introduction, 34.1
joint claims, 34.3.3
mergers, acquisitions and investments, 34.6.3
multi-party litigation
collective redress schemes, 34.3.7
competition law claims, 34.3.6
FOS/BBRS complaints, 34.3.5
group litigation orders, 34.3.2
introduction, 34.3
joint claims, 34.3.3
representative actions, 34.3.1
test cases, 34.3.4
other private litigation
arbitration, 34.6.5
civil law bribery, 34.6.1
data security breaches, 34.6.7
defamation proceedings, 34.6.4
employment law, 34.6.6
mergers, acquisitions and investments, 34.6.3
specific provisions in commercial contracts, 34.6.2
'tainted' contracts, 34.6.1
whistleblowing, 34.6.6
practical considerations, 34.8
privilege waivers and disclosure obligations, 34.8.2
representative actions, 34.3.1
resolving parallel investigations
foreign authorities, 23.5.2
introduction, 23.5
other domestic authorities, 23.5.1
securities litigation, 34.5
stay of proceedings
arbitral proceedings, 34.2.2
civil proceedings, 34.2.1
introduction, 34.2
'tainted' contracts, 34.6.1
test cases, 34.3.4
unfair prejudice petitions
generally, 34.4.2
practical considerations, 34.4.3
whistleblowing, 34.6.6

Parallel civil proceedings (US)
business events likely to give rise to parallel litigation, 35.5.3
business torts, 35.3.3.2
class actions
arbitration agreements, 35.3.1.5
opt-outs, 35.3.1.6
overview, 35.3.1.1
procedure, 35.3.1.3
public records as basis for filing, 35.3.1.2
standards, 35.3.1.3
statutory reforms, 35.3.1.4
conclusion, 35.6

© Law Business Research 2021

concurrent settlements, 35.5.2
contract claims, 35.3.3.1
coordination with internal investigations team, 35.5.1
derivative actions
indemnification and advancement, 35.3.2.3
overview, 35.3.2.1
procedure, 35.3.2.2
standards, 35.3.2.2
employment claims, 35.3.3.4
evidence
collateral use of disclosed documents, 35.4.3
introduction, 35.4
privilege waivers and disclosure obligations, 35.4.4
reliance by civil litigants on regulatory findings, 35.4.1
reliance by regulators on court findings, 35.4.2
insurance, 35.5.4
introduction, 35.1
practical considerations, 35.5
privilege waivers and disclosure obligations, 35.4.4
resolving parallel investigations
foreign authorities, 24.6.2
other domestic authorities, 24.6.1
statutory claims, 35.3.3.3
stay of proceedings
introduction, 35.2
protecting exercise of privilege against self-incrimination, 35.2.2
standard, 35.2.1
whistleblowing, 35.3.3.4

Penalties
see **Corporate penalties (UK)**; **Corporate penalties (US)**; **Individual penalties (UK)**; **Individual penalties (US)**

Pensions Regulator
production of documents/information, 11.2.5

Politics and political agendas
extradition, 32.3.3
risk management, 2.2.2.3

Pool counsel
generally, 16.2.2

Press
see **Media**

Privilege against self-incrimination
UK, 7.12
US, 16.5

Privilege (UK)
common interest privilege, 36.5
defending challenges to privilege
substantiating claims to privilege, 36.9.4
use of independent counsel, 36.9.5
employees
communications using employer email, 13.4.2
communications with colleagues or people involved in underlying events, 13.4.1.1
communications with company counsel, 13.4.1.2
ESG investigations, 47.4.3
exceptions
crime/fraud exception, 36.7.1
statutory and other exceptions, 36.7.2
inadvertent disclosure of privileged material, 36.8.3
introduction, 36.1
legal advice privilege
communications, 36.3.1
communications with multiple addressees, 36.3.4
definition of 'client', 36.3.2.2
definition of 'lawyer', 36.3.2.1
dominant purpose, 36.3.3
introduction, 36.3
legal professional privilege
adverse inferences, 36.2.4
global settlements, 23.3.1
introduction, 36.2
need for confidentiality, 36.2.1

© Law Business Research 2021

privilege belongs to client, 36.2.5
rationale, 36.2.3
substantive right, 36.2.2
litigation privilege
communications or other documents, 36.4.1
dominant purpose, 36.4.3
introduction, 36.4
litigation commenced or in contemplation, 36.4.2
loss of privilege, 36.8
maintaining privilege
conducting interviews, 36.9.1
introduction, 36.9
limitation of waivers, 36.9.2
redaction of documents, 36.9.3
production of documents/information, 11.4
publicity, tension with, 38.5.5
redaction of documents, 36.9.3
self-reporting
authorities' involvement in internal investigations, 3.7.2.4
legal advice in relation to internal investigations, 3.7.2.1
material generated during internal investigations, 3.7.2.2
waiver of privilege, 3.6.1.3, 3.7.2.3
Serious Fraud Office, 9.3.7
waiver
collateral waiver, 36.8.2
generally, 36.8
inadvertent disclosure of privileged material, 36.8.3
limitation, 36.9.2
limited waiver, 36.8.1
parallel civil proceedings, 34.8.2
without prejudice privilege, 36.6
witness interviews, 7.11

Privilege (US)
attorney work-product, 37.1.2
attorney–client privilege, 37.1.1
common interest privilege, 37.1.3
crime/fraud exception, 37.1.1
cross-border investigations, 18.5.1
disclosure to third parties
disclosure to company's auditors, 37.7.1
disclosure to foreign governments, 37.7.2
generally, 37.7
employees, 14.7, 37.3.1
ESG investigations, 47.4.3
expert witnesses, 37.8
former employees, 37.3.2
identifying the client, 37.2
inadvertent disclosure of privileged material, 37.4.2
joint defence privilege, 37.1.3
maintaining privilege
employee interviews, 37.3.1
former employees, 37.3.2
non-legal advice, 37.3.3
non-legal advice, 37.3.3
production of documents/information, 11.4
taint teams, 37.6
Upjohn warnings, 8.3, 37.3.1
waiver
co-operation credit, 37.4.1
generally, 37.4
inadvertent disclosure of privileged material, 37.4.2
parallel civil proceedings, 35.4.4
selective waiver, 37.5
witness interviews
note-taking, 8.5
Upjohn warnings, 8.3, 37.3.1
work-product and attorney–client privilege, 8.4

Probation
individual penalties, 31.2.4

Production of documents/information
conclusion, 11.5.6
cross-border investigations (UK)
Brexit, 11.5.3
information outside UK, 11.5.2
introduction, 11.5.1
requests into UK, 11.5.4

© Law Business Research 2021

cross-border investigations (US), 11.5.5
FCA and PRA
compulsory requests, 11.2.3.1
FCA/PRA obligations, 11.2.3.3
voluntary production, 11.2.3.2
Information Commissioner's Office, 11.2.4
in-house considerations
conclusion, 12.7
data collection and review, 12.3
initial considerations, 12.2
introduction, 12.1
material held overseas, 12.6
obtaining material from employees, 12.5
principal concerns, 12.4
introduction, 11.1
Pensions Regulator, 11.2.5
privilege, 11.4
regulators (UK)
FCA and PRA, 11.2.3
Information Commissioner's Office, 11.2.4
other authorities, 11.2.2
Pensions Regulator, 11.2.5
SFO, 11.2.1
regulators (US)
generally, 11.3
voluntary production, 11.3.1
SFO powers, 11.2.1
voluntary production
UK, 11.2.3.2
US, 11.3.1

Prudential Regulation Authority
production of documents/information
compulsory requests, 11.2.3.1
PRA obligations, 11.2.3.3
voluntary production, 11.2.3.2
Rules
approved persons, 19.3.1.3
Individual Conduct Rules, 19.3.1.1
introduction, 19.3.1
Senior Manager Conduct Rules, 19.3.1.2
self-reporting, 3.4.4
systems and controls requirements
internal whistleblowing arrangements, 19.2.4.1
introduction, 19.2.4
settlement agreements with workers, 19.2.4.3
whistleblowers' champion, 19.2.4.2

Public relations
see also **Media**
UK
determining remit of PR team, 38.2.2
identifying a PR team, 38.2.1
US, 39.1.5

Publicity (UK)
after commencement of investigation/prosecution
external actions and communications, 38.3.2
internal actions and communications, 38.3.1
after conclusion of investigation/prosecution
communications with prosecuting authorities, 38.4.1
debriefing, 38.4.2
before commencement of investigation/prosecution
determining remit of PR team, 38.2.2
identifying a PR team, 38.2.1
self-reporting, 38.2.4
tabletop exercises, 38.2.3
data protection, 38.5.4
ESG investigations, 47.4.3
introduction, 38.1
open justice
derogations, 38.5.1.2
generally, 38.5.1.1
remote hearings, 38.6
privilege, tension with, 38.5.5
public access to court documents/information, 38.5.3
public relations team

© Law Business Research 2021

determining remit, 38.2.2
identifying a team, 38.2.1
remote hearings, 38.6
reporting restrictions in criminal proceedings
automatic restrictions, 38.5.2.2
deferred prosecution agreements, 38.5.2.3
discretionary restrictions, 38.5.2.3
generally, 38.5.2.1
preparatory hearings, 38.5.2.3
prosecution appeals, 38.5.2.3
public access to court documents/information, 38.5.3
strict liability rule, 38.5.2.3
Publicity (US)
ESG investigations, 47.4.3
restrictions in criminal investigation or trial
consulting PR experts, 39.1.6
covid-19 impact, 39.1.5
discovery of internal corporate communications, 39.1.4
introduction, 39.1.1
investigatory and pretrial stage, 39.1.2
trial and post-trial stage, 39.1.3
rewards, 39.3.2
risks, 39.3.1
social media and the press
evidence, 39.2.1
investigative tools, 39.2.1
juries, 39.2.2

***Qui tam* actions**
effects of filing, 20.4.2
introduction, 20.4
procedure, 20.4.1

Racketeer Influenced and Corrupt Organizations Act
corporate penalties, 26.7.4
extraterritoriality, 29.4
Redaction of documents
generally, 36.9.3
Remote investigations
generally, 2.3
witness interviews, 8.8
Reporting restrictions
UK
automatic restrictions, 38.5.2.2
deferred prosecution agreements, 38.5.2.3
discretionary restrictions, 38.5.2.3
generally, 38.5.2.1
preparatory hearings, 38.5.2.3
prosecution appeals, 38.5.2.3
public access to court documents/information, 38.5.3
strict liability rule, 38.5.2.3
US
consulting PR experts, 39.1.6
covid-19 impact, 39.1.5
discovery of internal corporate communications, 39.1.4
introduction, 39.1.1
investigatory and pretrial stage, 39.1.2
trial and post-trial stage, 39.1.3
Representation in interviews (UK)
covid-19, 15.5
employees
interviewing client, 13.2.1.1
joint defence agreements, 13.2.2
requesting documents and information, 13.2.1.2
internal investigations
advising employee whether to attend, 15.2.3
lawyer's role in interview, 15.2.4
lawyer's role prior to interview, 15.2.2
when employees need own lawyer, 15.2.1
introduction, 15.1
law enforcement (suspect interviews)
cautions, 15.4.1
deciding on approach to take, 15.4.2
lawyer's role, 15.4.3

© Law Business Research 2021

law enforcement (witness interviews)
compulsory interviews, 15.3.2
confidentiality of interviews, 15.3.4
introduction, 15.3
right to representation, 15.3.3
voluntary interviews, 15.3.1
Representation in interviews (US)
conclusion, 16.6
decision to be interviewed
government investigations, 16.3.2
internal investigations, 16.3.1
employees
generally, 16.2.1
interviews without employee's counsel, 14.3.1
right to representation, 14.3
separate representation arranged for by employer, 14.3.2
introduction, 16.1
joint defence agreements, 16.2.3
kinds and scope of representation
generally, 16.2
joint defence agreements, 16.2.3
pool counsel, 16.2.2
representing current or former employees, 16.2.1
pool counsel, 16.2.2
preparation, 16.4
procedures for government interviews, 16.5
Representative actions
parallel civil proceedings, 34.3.1
Restitution orders
corporate penalties, 25.14
Restraint orders
corporate penalties, 25.9
cross-border investigations, 17.3.1
RICO
corporate penalties, 26.7.4
extraterritoriality, 29.4
Risk management
compliance function's role, 2.5
ESG investigations, 2.4, 47.4.5
external investigations
contact by authorities, 2.2.2.1
customer and competitor complaints, 2.2.2.5
investor complaints, 2.2.2.4
media coverage, 2.2.2.2
politics and political agendas, 2.2.2.3
shareholder derivative lawsuits, 2.2.2.4
internal investigations
audits and reviews, 2.2.1.2
internal whistleblowers, 2.2.1.1
transactional due diligence, 2.2.1.3
introduction, 2.1
legal function's role, 2.5
remote investigations, 2.3
sources and triggers for investigations, 2.2

Sanctions (UK)
best practices in investigations
co-operation, 44.5.2
factors to consider, 44.5.1
self-reporting, 44.5.2.1
settlement, 44.5.3
exemptions, 44.2.3
introduction, 44.1
investigations, 44.4
key jurisdictions
introduction, 44.2.4
Iran, 44.2.4.1
North Korea, 44.2.4.2
Russia/Ukraine, 44.2.4.3
licensing, 44.2.3
offences and penalties
civil penalties, 44.3.2
criminal penalties, 44.3.1
introduction, 44.3
prosecutions, 44.3.1
official guidance, 44.2.1
persons to whom sanctions apply, 44.2.2
potential pitfalls, 44.6.2
recent enforcement activity, 44.6.1
sanctions regime, 44.2
statutes, 44.2

© Law Business Research 2021

Sanctions (US)
best practices in investigations
introduction, 45.4.3
self-reporting to DOJ, 45.4.3.2
self-reporting to OFAC, 45.4.3.1
settlement, 45.4.3.3
enforcement
best practices, 45.4.3
compliance framework, 45.4.2
factors to consider, 45.4.1
recent enforcement activity, 45.5.1
introduction, 45.1
investigations, 45.3
key jurisdictions
Crimea region of Ukraine, 45.1.4.5
Cuba, 45.1.4.1
introduction, 45.1.4
Iran, 45.1.4.2
North Korea, 45.1.4.3
Russia, 45.1.4.6
Syria, 45.1.4.4
Venezuela, 45.1.4.7
licensing, 45.1.3
offences and penalties, 45.2
official guidance, 45.1.1
persons to whom sanctions apply, 45.1.2
potential pitfalls, 45.5.2
recent enforcement activity, 45.5.1
sanctions regime, 45.1
statutes, 45.1.1
Sarbanes-Oxley Act
whistleblowing, 20.1.1
Scope of internal investigations
UK, 5.5
US
developing a work plan, 6.5.3
identifying necessary partners, 6.5.2
introduction, 6.5
key documents and scoping interviews, 6.5.1
Securities litigation
parallel civil proceedings, 34.5
Seizure
see **Asset recovery (UK)**; **Asset recovery (US)**
Self-incrimination
UK, 7.12
US, 16.5
Self-reporting to authorities (UK)
see also **Co-operation with authorities (UK)**
advantages
co-operation credit, 3.6.1
demonstration of culture and strength of systems and controls, 3.6.3
information control, 3.6.4
leniency or penalty reduction, 3.6.2
co-operation credit
continuing co-operation, 3.6.1.2
generally, 3.6.1
timing of self-reporting, 3.6.1.1
waiver of privilege, 3.6.1.3
culture, 3.2
data security breaches, 3.4.2
decision to self-report
clear communication, 3.8.1.1
clear protocol and structure, 3.8.1.3
documenting the decision, 3.8.2.1
even, dispassionate investigation, 3.8.1.2
introduction, 3.8.1
senior management involvement, 3.8.1.4
deferred prosecution agreements
evolution of link with self-reporting, 3.3
reporting obligations, 3.4.3
timing, 3.6.1.1
Financial Conduct Authority, 3.4.4
financial sanctions breaches, 3.4.2
introduction, 3.1
managing other regulators, 3.8.3
money laundering, 3.4.1
other reporting obligations, 3.4.2
practical considerations
decision to self-report, 3.8.1

© Law Business Research 2021

documenting the decision, 3.8.2.1
managing other regulators, 3.8.3
nature of approach to authorities, 3.8.2.2
steps after decision made, 3.8.2
timing of self-report, 3.8.2.3
private agreements, 3.4.3
privilege
authorities' involvement in internal investigations, 3.7.2.4
legal advice in relation to internal investigations, 3.7.2.1
material generated during internal investigations, 3.7.2.2
waiver, 3.6.1.3, 3.7.2.3
Prudential Regulation Authority, 3.4.4
regulatory agreements, 3.4.3
risks
generally, 3.7
impact on witness interviews, 3.7.3
interest and potential investigation in other jurisdictions, 3.7.1
potential monitoring obligations, 3.7.4
privilege issues, 3.7.2
scrutiny, 3.7.4
sectoral reporting obligations, 3.4.2
Serious Fraud Office, 3.5
sharing information by regulators, 3.8.3
terrorist financing, 3.4.1
timing, 3.8.2.3
whistleblowing, 3.2
Self-reporting to authorities (US)
see also **Co-operation with authorities (US)**
introduction, 4.1
mandatory self-reporting
introduction, 4.2
obligations under agreements with government, 4.2.2
other sources of obligations, 4.2.3
statutory and regulatory obligations, 4.2.1
voluntary self-reporting
advantages, 4.3.1
Benczkowski Memorandum, 4.3.1.1
co-operation credit (DOJ), 4.3.1.1
co-operation credit (SEC), 4.3.1.2
Corporate Enforcement Policy, 4.3.1.1
introduction, 4.3
risks in not self-reporting, 4.5
risks in self-reporting, 4.4
Yates Memorandum, 4.3.1.1
Serious crime prevention orders
corporate penalties, 25.10
Serious Fraud Office
see also **Co-operation with authorities (UK)**; **Self-reporting to authorities (UK)**
compliance programmes, 1.3.4
privilege, 9.3.7
production of documents/information, 11.2.1
whistleblowing, 19.2.6
Settlement
see **Global settlements (UK)**; **Global settlements (US)**
Shareholder derivative claims
see **Derivative claims**
Social issues
see **Environmental, social and governance investigations**
Social media
publicity (UK), 38.1
publicity (US)
investigative/evidential tool, 39.2.1
juries, 39.1.3, 39.2.2
Stages of investigations
commencement, 1.3.1
compliance programmes, 1.3.4
disposal, 1.3.3
information gathering, 1.3.2
introduction, 1.3
Stay of proceedings
UK
arbitral proceedings, 34.2.2

© Law Business Research 2021

civil proceedings, 34.2.1
introduction, 34.2
US
introduction, 35.2
protecting exercise of privilege against self-incrimination, 35.2.2
standard, 35.2.1

'Tainted' contracts
parallel civil proceedings, 34.6.1
Tax evasion
extraterritoriality, 28.4
Terms of reference
see **Scope of internal investigations**
Terrorist financing
self-reporting, 3.4.1
Test cases
parallel civil proceedings, 34.3.4
Third-party rights
UK, 30.3
US, 31.2.6
Tolling agreements
global settlements, 24.3.2
Transactional due diligence
risk management, 2.2.1.3

UN Guiding Principles on Business and Human Rights
ESG investigations, 47.3.2.1
Unexplained wealth orders
individual penalties, 30.1.3
Unfair prejudice petitions
generally, 34.4.2
practical considerations, 34.4.3
***Upjohn* warnings**
employee interviews, 8.3, 37.3.1

Vicarious liability
UK, 1.1.1, 19.2.1.4
US, 1.1.2
Victim restitution
UK
corporate penalties, 25.2, 25.14
individual penalties, 30.1.5
US, 31.2.6

Waiver of privilege
UK
collateral waiver, 36.8.2
generally, 36.8
inadvertent disclosure of privileged material, 36.8.3
limitation, 36.9.2
limited waiver, 36.8.1
parallel civil proceedings, 34.8.2
US
co-operation credit, 37.4.1
generally, 37.4
inadvertent disclosure of privileged material, 37.4.2
parallel civil proceedings, 35.4.4
selective waiver, 37.5
Whistleblowing (UK)
automatically unfair dismissal, 19.2.1.2
Competition and Markets Authority, 19.2.5
corporate perspective
anonymity protection, 19.3.4.1
Bribery Act 2010, 19.3.2.1
changing regulatory expectations, 19.3.3
conduct of investigation, 19.3.4.2
Criminal Finances Act 2017, 19.3.2.2
cross-border considerations, 19.3.4.5
data protection, 19.3.4.3
effective reporting channels, 19.3.4.1
FCA/PRA Rules, 19.3.1
interaction with regulatory obligations, 19.3.4.4
listed companies, 19.3.4.4
practical considerations, 19.3.4
Principle 11/Fundamental Rule 7, 19.3.4.4
Proceeds of Crime Act 2002, 19.3.4.4

© Law Business Research 2021

territorial application of UK legislation, 19.3.4.5
data protection
corporate perspective, 19.3.4.3
cross-border data transfers, 19.3.4.5
introduction, 40.6
right to access data, 40.6.2
whistleblowing policies, 40.6.1
detriment, 19.2.1.1
Employment Rights Act 1996
automatically unfair dismissal, 19.2.1.2
generally, 19.2.1
qualifying disclosures, 19.2.1.3
unlawful detriment, 19.2.1.1
vicarious and personal liability, 19.2.1.4
FCA/PRA Rules
approved persons, 19.3.1.3
Individual Conduct Rules, 19.3.1.1
introduction, 19.3.1
Senior Manager Conduct Rules, 19.3.1.2
FCA/PRA systems and controls requirements
internal whistleblowing arrangements, 19.2.4.1
introduction, 19.2.4
settlement agreements with workers, 19.2.4.3
whistleblowers' champion, 19.2.4.2
human rights, 19.2.7
individual perspective
challenges to unfair treatment, 19.4.4.3
immunity from prosecution, 19.4.2
legal risks of whistleblowing, 19.4.1
leniency, 19.4.2
practical considerations, 19.4.4
professional obligations, 19.4.3
requests to sign NDA, 19.4.4.2
to whom to blow the whistle, 19.4.4.1
in-house perspective
covid-19, 21.5
distinctive aspects of investigations, 21.4
employee approaches, 21.3
EU Whistleblower Directive, 21.6
identifying legitimate claims, 21.2
initial considerations, 21.1
ISO Whistleblowing Management Systems, 21.7
introduction, 19.1
legal framework
Competition and Markets Authority, 19.2.5
Employment Rights Act 1996, 19.2.1
EU Whistleblower Directive, 19.2.2
FCA/PRA systems and controls requirements, 19.2.4
human rights, 19.2.7
legislative proposals, 19.2.2
non-disclosure agreements, 19.2.3
Public Interest Disclosure Act 1998, 19.2.1
Serious Fraud Office, 19.2.6
non-disclosure agreements, 19.2.3, 19.4.4.2
parallel civil proceedings, 34.6.6
personal liability, 19.2.1.4
qualifying disclosures, 19.2.1.3
risk management
external whistleblowers, 2.2.2.5
internal whistleblowers, 2.2.1.1
self-reporting, 3.2
Serious Fraud Office, 19.2.6
vicarious liability, 19.2.1.4
Whistleblowing (US)
anti-retaliation suits
SEC suits, 20.2.4
whistleblower suits, 20.2.3
CFTC regime, 20.1.2
corporate perspective
defending anti-retaliation suits, 20.2.3

© Law Business Research 2021

preparing for whistleblower report, 20.2.1
responding to whistleblower report, 20.2.2
SEC anti-retaliation suits, 20.2.4
disclosure to SEC, 20.3.1
individual perspective
awards under DFA, 20.3.2
disclosure to SEC, 20.3.1
generally, 20.3
recent awards, 20.3.3
in-house perspective
covid-19, 21.5
distinctive aspects of investigations, 21.4
employee approaches, 21.3
EU Whistleblower Directive, 21.6
identifying legitimate claims, 21.2
initial considerations, 21.1
ISO Whistleblowing Management Systems, 21.7
overview of statutes, 20.1
parallel civil proceedings, 35.3.3.4
qui tam actions under False Claims Act
effects of filing, 20.4.2
introduction, 20.4
procedure, 20.4.1
risk management
external whistleblowers, 2.2.2.5
internal whistleblowers, 2.2.1.1
Sarbanes-Oxley Act, 20.1.1
SEC regimes, 20.1.1
state law regimes, 20.1.3

Withdrawal of authorisation
corporate penalties, 25.12

Without prejudice privilege
generally, 36.6

Witness interviews (UK)
see also **Representation in interviews (UK)**
conducting interviews
cautions, 7.9
employee amnesty and self-incrimination, 7.12
formalities and separate counsel, 7.8
legal privilege, 7.11
record-keeping, 7.10
consultation with authorities, 7.3
employees abroad, 7.14
former employees, 7.13
identifying witnesses, 7.5
introduction, 7.1
key points, 7.15
legal privilege, 7.11
monitors, 33.5.4
order of interviews, 7.5
planning, 7.7
providing details of interviews to authorities, 7.4
timing, 7.6
types of interview, 7.2

Witness interviews (US)
see also **Representation in interviews (US)**
attorney–client privilege, 8.4
conclusion, 8.10
document review and selection, 8.7
interactions with witnesses, 8.6
introduction, 8.1
monitors, 32.5.4
note-taking, 8.5
preparation, 8.2
privilege
note-taking, 8.5
Upjohn warnings, 8.3, 37.3.1
work-product and attorney–client privilege, 8.4
remote interviews, 8.8
reporting results, 8.9
Upjohn warnings, 8.3, 37.3.1
work-product privilege, 8.4

Work plans
development, 6.5.3
monitorship, 32.5.3

Work-product
privilege, 8.4, 37.1.2

© Law Business Research 2021

GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

SIXTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2021

© Law Business Research 2021

The Practitioner's Guide to Global Investigations

Volume II: Global Investigations around the World

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2021
For further information please contact insight@globalinvestigationsreview.com

© Law Business Research 2021

The Practitioner's Guide to Global Investigations

Sixth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Celeste Koeleveld

© Law Business Research 2021

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK
© 2020 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
natalie.hacker@lbresearch.com
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-272-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© Law Business Research 2021

Acknowledgements

Addleshaw Goddard LLP

Anagnostopoulos

Association of Corporate Investigators

Baker McKenzie LLP

BCL Solicitors LLP

BDO USA, LLP

Borden Ladner Gervais LLP

Brown Rudnick LLP

Cadwalader, Wickersham & Taft LLP

Claro y Cia

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Corker Binning

Cravath, Swaine & Moore LLP

Debevoise & Plimpton LLP

DLA Piper LLP

Fornari e Associati

Fountain Court Chambers

Fox Williams LLP

Freshfields Bruckhaus Deringer

Gleiss Lutz

Goodwin

Gün + Partners

Herbert Smith Freehills LLP

© Law Business Research 2021

Homburger

JAMES P LOONAM ESQ

Jenner & Block

Kingsley Napley LLP

Latham & Watkins

Law Offices of Panag and Babu

Linklaters LLP

Marval O'Farrell Mairal

Matheson

Mayer Brown

McGuireWoods

Mishcon de Reya LLP

Navacelle

Norton Rose Fulbright LLP

Outer Temple Chambers

Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pinsent Masons LLP

Rajah & Tann Singapore LLP

Rebaza, Alcázar & De Las Casas

Reed Smith LLP

Ropes & Gray LLP

Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Slaughter and May

Sofunde Osakwe Ogundipe & Belgore

Sullivan & Cromwell LLP

Trench Rossi Watanabe

Uría Menéndez Abogados, SLP

Von Wobeser y Sierra, SC

Walden Macht & Haran LLP

Willkie Farr & Gallagher LLP

© Law Business Research 2021

Contents

Introduction to Volume II 1
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Celeste Koeleveld

PART I: REGIONAL OVERVIEWS

1 Asia-Pacific Overview 5
Kyle Wombolt and Pamela Kiesselbach

2 Europe Overview 14
Robert Dalling, Kelly Hagedorn and Matthew Worby

3 Latin America Overview 26
María González Calvet

4 North America Overview 47
John D Buretta

PART II: INVESTIGATIONS COUNTRY BY COUNTRY

5 Argentina 63
Gustavo Morales Oliver and María Lorena Schiariti

6 Australia 85
Tim Grave and Lara Gotti

© Law Business Research 2021

7 Brazil 113
Heloísa Barroso Uelze, Felipe Noronha Ferenzini and João Augusto Gameiro

8 Chile 137
Alex van Weezel and Santiago Breton

9 China 162
Kyle Wombolt, Helen Tang and Tracey Cui

10 Colombia 190
Pamela Alarcón Arias

11 France 214
Stéphane de Navacelle and Julie Zorrilla

12 Germany 240
Eike Bicker, Christian Steinle, Christoph Skoupil and Marcus Reischl

13 Greece 263
Ilias Anagnostopoulos, Jerina Zapanti and Alexandros Tsagkalidis

14 Hong Kong 286
Donna Wacker, Jonathan Wong, Anita Lam, William Wong and Michael Wang

15 Ireland 317
Karen Reynolds, Connor Cassidy and Noel Power

16 Italy 346
Enrico Di Fiorino and Lorena Morrone

17 New Zealand 368
William Fotherby, Britt Rorrison and Caitlin Anyon-Peters

© Law Business Research 2021

18 Peru 395
Alberto Rebaza, Augusto Loli, Héctor Gadea, María Haydée Zegarra and Sergio Mattos

19 Poland 415
Marcin Ciemiński, Paweł Pogorzelski, Monika Diehl and Michał Magdziak

20 Russia 439
Hannes Lubitzsch

21 Singapore 463
Kabir Singh, Janice Goh and Tian Yi Tan

22 Spain 487
Jaime Alonso Gallo and Sara Sanz Castillo

23 Switzerland 511
Flavio Romerio, Claudio Bazzani, Katrin Ivell and Reto Ferrari-Visca

24 United Kingdom 537
Tom Stocker, Neil McInnes, Natalie Sherborn, Andrew Sackey, Laura Gillespie and Olga Tocewicz

25 United States 585
Bradley J Bolerjack, Francisca M Mok, Eric H Sussman and Jennifer L Achilles

Appendix 1: About the Authors of Volume II 607
Appendix 2: Contributors' Contact Details 635

© Law Business Research 2021

Introduction to Volume II

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Celeste Koeleveld[1]

Boards and senior executives have never been more concerned that they or their organisation may come under the scrutiny of enforcement authorities. And with good reason. Recent years have seen an upsurge in confidence among enforcement authorities across the globe, which has manifested and led to increased numbers of investigations, fines of unprecedented orders of magnitude and senior executives facing the much more realistic prospect of investigations concerning their own conduct and, in some cases, prosecution, conviction and imprisonment.

In many jurisdictions, the introduction of new offences and changes to the law of corporate criminal liability have provided enforcement authorities with increased opportunities to pursue criminal investigations and ultimately to prosecute corporate entities. Coupled with this has been the incentivisation of corporates to co-operate with investigations and provide information to assist authorities in pursuing culpable individuals through negotiated settlements. In some jurisdictions, notably the United States, co-operation is an established feature of the enforcement landscape and is regularly used to bring investigations to a pragmatic conclusion without the commercially destructive consequences that prosecution of a corporate entity can bring. In others, such as the United Kingdom and France, legislation enabling corporates to conclude investigations short of prosecution is still comparatively young, although significant settlements involving multinationals have demonstrated the abilities of enforcement authorities to reach outside their own jurisdictions and to coordinate to an ever greater extent.

The law relating to criminal and regulatory investigations shows no sign of standing still. Law and practice across the globe have changed, often in response to highly publicised

1 Judith Seddon and Ama A Adams are partners at Ropes & Gray LLP; Christopher J Morvillo, Luke Tolaini and Celeste Koeleveld are partners at Clifford Chance; Eleanor Davison is a barrister at Fountain Court Chambers; and Michael Bowes QC is a barrister at Outer Temple Chambers.

© Law Business Research 2021

scandals. Relationships between enforcement authorities continue to grow closer and there is a marked trend in politicians, prosecutors and regulators carefully watching the way other jurisdictions choose to combat corporate crime, as they assess the most effective mechanisms to apply in their own national contexts. Recent examples of changes to legislation in terms of either extending corporate criminal liability or legislating for its resolution through deferred prosecution agreements (or both) include significant changes being enacted in Germany, Malaysia, Norway and Australia.[2] A similar trend may be observed in the regulatory sphere through the implementation of individual accountability regimes modelled on or drawing from the UK Senior Managers and Certification Regime in, for example, Hong Kong, Australia and Singapore.

All these macro factors, with some important changes to technical local legislation (e.g., the EU General Data Protection Regulation), present numerous, significant challenges to corporates and individuals around the world. They can quickly find themselves the target of fast-moving and far-reaching investigations, whose possible outcomes may vary significantly in different jurisdictions.

Volume II of this Guide covers 21 jurisdictions in this edition and includes overviews of four regions: Asia-Pacific, Europe, Latin America and North America. Local experts from each national jurisdiction respond to a common set of questions designed to identify the local – continually evolving – nuances of law and process that practitioners are likely to encounter in responding to the increasing number of cross-border investigations they face.

2 In Germany, the Ministry of Justice has published a draft bill intended to extend corporations' liability for certain actions of their executive bodies and employees. The bill failed in 2021, but may be introduced again. Malaysia has introduced corporate liability for corruption offences and there are calls for the introduction of deferred prosecution agreements for companies. Norway has extended corporate criminal liability for certain corruption offences committed by Norwegian companies outside Norway. In December 2019, the Australian Federal Government introduced the Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019 (Cth) (CLACCC Bill), which, if enacted, would introduce a new offence of failure to prevent bribery of a foreign public official and a deferred prosecution regime. In April 2020, the Australian Law Reform Commission issued a Report on Corporate Criminal Responsibility – which included consideration of the CLACCC Bill – and made recommendations to Parliament for further reform of corporate criminal liability. The Bill is still being considered.

© Law Business Research 2021

Part I

Regional Overviews

© Law Business Research 2021

1

Asia-Pacific Overview

Kyle Wombolt and Pamela Kiesselbach[1]

Introduction

The region has witnessed significant corporate investigations, substantive legal reform and aggressive enforcement in recent years. Although legislative developments and enforcement have been slowed down by the effect that covid-19 has had on the operation of government departments, the general trends of recent years are continuing. The Banking Royal Commission in Australia, corporate criminal liability provisions inspired by the UK Bribery Act across several jurisdictions in Asia and the omnipresent focus of the US Department of Justice (US DOJ) on China mean that companies in the region continue to face clear business risk. At the same time, covid-19 has resulted in an uptick in criminal activity in certain areas, such as money-laundering, cyber-related crimes and corruption. For example, the Australian Competition and Consumer Commission reported in June 2020 that business email compromise scams have caused the highest losses of all types of scams. This is a trend that has been replicated in other Asia-Pacific countries, such as China and Hong Kong, Thailand, Malaysia and Singapore, resulting in the theft of hundreds of millions of US dollars. And although the continued effects of the United States cannot be underplayed, national authorities continue to demonstrate an appetite for investigating and prosecuting large cases themselves. Partly as a result of this, there is a sustained increase in complex, multi-jurisdictional investigations. This highlights a further regional trend – increased co-operation between regulators in different jurisdictions. On a practical level, enhanced information sharing requires a coordinated response by investigated parties to manage competing requests for information, determine appropriate remedial steps and ultimately find solutions to conclude multiple investigations. In a region that combines civil law and common law jurisdictions, it is

1 Kyle Wombolt is a partner and Pamela Kiesselbach is a senior consultant (England and Wales) at Herbert Smith Freehills. The information in this chapter was correct as at November 2020.

© Law Business Research 2021

not surprising to find different approaches to data privacy and legal privilege. However, the challenges that this poses have been exacerbated by the introduction of a number of blocking statutes in China, prohibiting individuals and entities from providing information to criminal enforcement and regulatory authorities outside the country without the approval of Chinese authorities. This can lead to challenges for corporates and their advisers when conducting internal investigations and responding to external regulatory investigations. In this chapter, we highlight some of the overarching themes and developments that we have been seeing.

Areas of enforcement risk

Bribery and corruption remain core areas for law enforcement, with domestic and international agencies homing in on conduct in the region. National anti-corruption agencies in Australia, Indonesia, Malaysia and China have all bolstered their powers of investigation and oversight. In tandem, some governments (such as in Australia and China) have introduced more stringent corporate penalties. In terms of international enforcement, misconduct in China has long been the subject of more corporate bribery investigations under the US Foreign Corrupt Practices Act than any other jurisdiction. The US DOJ continues to pursue its China Initiative. This focuses on Chinese companies' outbound activity and reflects the United States' desire to pursue prosecution when Chinese companies' offshore activities affect US national interests. Having said this, China's focus on corruption-related enforcement continues unabated and corruption convictions have nearly doubled in the past year.

Money laundering, tax evasion, (accounting) fraud, competition and cybercrime are other key areas for corporate investigations in the Asia-Pacific region.

Anti-money laundering (AML) and counter-terrorism financing (CTF) have been under the spotlight. Although some country evaluations scheduled by the Financial Action Task Force (FATF) for 2020 have been delayed because of the covid-19 pandemic (e.g., Japan), FATF has published material setting out particular risks and policy responses relevant to covid-19 with regard to money laundering and terrorism financing. It is clear that law enforcement agencies continue to prioritise AML/CTF efforts, although some have shifted their focus to emerging covid-19 predicate offences, which is evidenced by, among other things, relevant guidance published by criminal enforcement and regulatory authorities in China, Hong Kong and Singapore. Many jurisdictions, including Hong Kong, Singapore, Vietnam, India and China continue to ramp up domestic AML legislation and corporate enforcement. The region's focus on money laundering is best highlighted by hydra-styled investigations such as 1MDB,[2] which started in Malaysia but has spread to the highest levels of public office and corporate business globally, including world-famous banks. Governments are pursuing regulatory and criminal actions against financial and other institutions for their failure to implement sufficient controls to monitor global transactions. Banks, in particular, are subject to increasing scrutiny through audits, examinations, inspections and investigations. The Monetary Authority of Singapore (MAS) has been particularly active in revoking licences and imposing significant fines

2 1 Malaysia Development Berhad is an insolvent Malaysian strategic development company.

© Law Business Research 2021

during the past few years, and has continued to do so in 2020, including with regard to asset management and trust companies.

Tax evasion is another area in which there is heightened activity in the region. This has been led by the United States under its Foreign Account Tax Compliance Act and the aftermath of its Swiss bank programme, when the US DOJ announced that it would be following funds that are the subject of US tax evasion from Switzerland to financial centres in Asia, such as Hong Kong and Singapore. The pressure on taxpayers and financial institutions has been accelerated and broadened further by the Organisation for Economic Co-operation and Development's Common Reporting Standard. The 'follow the money' initiatives that are being pursued by a number of jurisdictions, including the United States, have highlighted Asian financial centres as targets. An Indonesian tax amnesty – the aim of which was repatriating off-shore funds – is another obvious example, as a vast majority of the funds were located with banks in Singapore. The upshot is a further focus on banks in the region, with authorities in India, Australia and New Zealand showing an appetite for reviewing tax-sharing information to root out corporate tax evasion, particularly through multilateral treaties to prevent base erosion and profit shifting.

Fraud, particularly tax and accounting fraud, continue to occupy law enforcement too. There are a number of recent high-profile examples, including Wirecard (across several Asia-Pacific countries) and Kangmei Pharmaceutical Co, one of China's biggest pharmaceutical companies. The latter resulted in the China Securities Regulatory Commission blacklisting six executives for their role in a US$4.2 billion accounting scandal.

Cybercrime has been a board-level issue for the past few years regardless of jurisdiction, but some of the biggest corporate investigations have touched on the Asia-Pacific region. Asia is considered relatively insecure in terms of infrastructure, meaning cyberattacks are more common. Singapore, one of the leading global digital economies, has become a target, particularly in the health sector. We have also seen a marked increase in state-sponsored cyberattacks, which has led to the first set of sanctions being introduced under the European Union's new cyber sanctions regime. The sanctions were imposed in relation to individuals and organisations in North Korea, China and Russia. In response, domestic authorities and regulators have increased compliance and reporting requirements. This turns up the temperature on corporates, who must be ready for internal and external investigations emanating from cybercrime.

A shift from individual to corporate liability

Historically, enforcement agencies in the Asia-Pacific region have focused on individual criminal liability in the context of public sector bribery, often concentrating on prosecuting the government officials receiving the bribes. However, there have been some clear shifts in focus, demonstrated by legislative changes and statements made by enforcement agencies. The most uniform shift in a number of Asia-Pacific jurisdictions relates to the introduction of corporate criminal liability and accountability of senior management. Thailand, India, Japan, Singapore, Malaysia, Indonesia and China have all introduced legislation, making it easier either to attach corporate criminal liability or to penalise companies involved in bribery. Australia continues to review its corporate criminal responsibility regime. India, Indonesia, Malaysia and Thailand were all inspired by the UK Bribery Act section 7 corporate offence in crafting their own legislation, and the corporate liability regime has come

© Law Business Research 2021

into effect most recently in Malaysia on 1 June 2020. In simple terms, under these often still fairly new rules, companies may be held criminally liable if their employees or agents or otherwise 'associated persons' commit bribery or other criminal offences while acting on behalf, or for the benefit, of the company. As is the case under the UK Bribery Act, these rules take into account whether a company had adequate procedures in place to prevent the criminal offence when determining the company's liability. Although some provisions are limited to bribery offences (e.g., in Malaysia and India), others are more broadly drafted to cover other criminal offences as well (e.g., in Indonesia). However, the new corporate criminal liability offence introduced in Vietnam covers tax evasion and money laundering offences and does not extend to bribery offences.

The corporate liability offences plug gaps in domestic regimes, give law enforcement and regulators greater powers, and ease the requirement of meeting the difficult threshold of showing involvement of the 'directing mind and will' of the company to establish corporate liability. Critically, there is increasing pressure on companies to put adequate procedures and controls in place to prevent bribery if they wish to escape liability for misconduct carried out by employees or agents when acting for the company.

The new corporate liability provisions in Malaysia and India make it clear that they cover foreign entities that carry on their business, or part of their business, in the jurisdiction. Indonesian laws go one step further and provide that a group company, including a parent or affiliate company, may be held criminally liable if it is considered to be involved in the bribery. As a result, companies operating in the region should ensure that appropriate internal control measures are in place or re-evaluate their measures so that they do comply with relevant domestic guidelines. The increased corporate exposure has also resulted in investors and, in some instances, lenders conducting heightened compliance-related due diligence on local companies before entering into a merger or a joint venture, or making an investment to gauge and manage their exposure.

Senior managers are also facing enhanced exposure to liability, putting their companies under additional compliance risk. A Senior Managers Regime, similar to the United Kingdom's Senior Managers' and Certification Regime, has been introduced in Hong Kong and Singapore to enable the financial sector to improve the individual accountability of senior managers. Anti-bribery provisions in Malaysian, Indian and Indonesian laws potentially extend criminal liability to senior management. This means that senior managers may be held liable for bribery committed under their watch when they are seen to have either proactively authorised or at least known of, and acquiesced in, bribery. Although largely untested at this stage, there is a risk that liability may be inferred when there is a suspicion of bribery and a senior manager does nothing to stop the bribery, or turns a blind eye to clear indications of bribery. Indonesian law potentially goes further, in that senior management may be held responsible for wrongdoing by employees or agents acting on behalf of a company simply based on their status.

Other trend shifts relate to broadening the focus to cover private sector bribery and supply-side bribery to an increasing extent. Notable illustrations of the former are the introduction of a private sector bribery offence in Vietnam and the fact that around 70 to 80 per cent of bribery-related prosecutions in Singapore and Hong Kong concern incidents within the private sector. Although public sector bribery is still considered to attract a higher level of enforcement risk, it is important not to lose sight of the criminality of

© Law Business Research 2021

private sector bribery. In jurisdictions that still 'only' provide for prohibitions on public sector bribery (e.g., India and Indonesia), the scope of who may be considered a public official is often extended. Further, recent legislative changes in India have introduced a supply-side bribery offence and officials at Indonesia's anti-graft body, the Corruption Eradication Commission (KPK), have been issuing statements indicating that they intend to focus more on those who give bribes and not just on the public officials receiving bribes.

Culture

Culture has become a central tenet of, and compliance imperative for, corporate investigations in the region. Banks in particular have been facing a culture and conduct storm. The Banking Royal Commission in Australia illustrates the role of corporate culture at the meso (organisation) and macro (industry) levels. Further, regulatory and stock exchange authorities in Hong Kong and Singapore (i.e., the Hong Kong Monetary Authority, the MAS, the Singapore Exchange Regulation and the Stock Exchange of Hong Kong Limited) have published consultation papers in May, July and August 2020, reaffirming the regulators' continued focus on culture and conduct, and keeping 'bad apples' out of financial institutions and public companies.

With most jurisdictions moving to disclosure-driven, risk-based systems, an assessment of corporate culture involves a top-down review to assess the readiness of a company to limit the occurrence of misconduct and its reaction to it once on notice. A failing corporate culture can be evidenced by any of the following: a lack of corporate policies and training, poor tone from the top, turning a blind eye, lack of personal accountability and express or tacit authorisation of poor conduct.

UK Bribery Act-inspired legislation in certain jurisdictions, particularly those with adequate procedures defences, highlights the growing relevance of corporate culture in Asia. Further, corporate culture continues to affect enforcement outcomes. For example, the US DOJ Criminal Division's updated Guidance on the Evaluation of Corporate Compliance Programs helps to benchmark the effectiveness of a company's compliance programme. The Guidance assists US authorities with decisions when conducting an investigation, determining whether to bring charges, or negotiating pleas or other arrangements. Whether in the United States, the Asia-Pacific region or elsewhere, the Guidance sets out useful prompts for a best practice compliance framework. Given the propensity of regulators to borrow from each other's procedures and practices, it will also be of interest to companies subject to regulatory scrutiny, investigation or enforcement outside the United States, as a benchmark for appropriate remediation and resolution.

Guidance has also been issued by the Prime Minister's Department in Malaysia, setting out anti-corruption programmes and procedures to be adopted by companies doing business in Malaysia. The guidance (which is similar to that issued in the United Kingdom under the Bribery Act 2010) describes an effective, risk-based compliance programme that minimises the risk of misconduct occurring and, where it does occur, mitigates the potential consequences for the company. However, when reviewing anti-corruption policies and procedures of listed companies, the Securities Commission Malaysia found that just under 60 per cent of listed companies had anti-corruption policies in place and most of these policies were not in line with the guidance.

© Law Business Research 2021

Information-sharing and multi-jurisdictional investigations

It is rare for an allegation into corporate misconduct to remain a domestic affair, such is the global nature of modern commerce and communication. Regulators are ramping up cross-border co-operation and resolutions in response. Some very high-profile corporate investigations demonstrate how concurrent multi-jurisdictional investigations are now the norm. It is noteworthy in this context that cross-border information sharing between authorities is often informal and will not always follow formal and time-consuming procedures under mutual legal assistance treaties.

An example of where local enforcement action has followed and built on enforcement by US or UK authorities (or both) is the *Rolls-Royce* matter, in which the settlement covered allegations that Rolls-Royce bribed officials in multiple countries for more than 20 years. The British company's alleged bribery of officials at airline company Garuda Indonesia and others was covered in the £671 million settlement that Rolls-Royce reached with the United Kingdom's Serious Fraud Office (SFO), the US DOJ and Brazil's Federal Prosecution Service in January 2017. Using information obtained from the SFO/US DOJ investigation, the KPK in Indonesia opened an investigation against several individuals at Garuda, including the company's former president and chief executive officer, Emirsyah Satar. Mr Satar was convicted of accepting illicit payments totalling US$1.5 million and other items worth US$2 million and was sentenced to eight years in prison in May 2020. Garuda has commenced civil proceedings against Rolls-Royce for compensation in the Indonesian courts. Indian authorities, including the Central Bureau of Investigation, have also opened an investigation into the use by Rolls-Royce of third-party intermediaries to win contracts. A similar pattern has been playing out involving allegations of corruption, involving Airbus and executives of the Malaysian airline, AirAsia. Airbus entered into a deferred prosecution agreement (DPA) at the beginning of 2020 involving authorities in the United Kingdom, the United States and France requiring Airbus to make payments totalling €3.6 billion. Shortly after that, the Malaysian Anti-Corruption Commission initiated an investigation against executives of AirAsia with regard to the alleged acceptance of bribes and has been in touch with the SFO seeking relevant information.

GlaxoSmithKline plc (GSK) is another famous example of a global brand being caught up in bribery in Asia, leading to investigations and charges in multiple jurisdictions. Between 2004 and 2010, GSK's sales teams in China were alleged to have bribed doctors to prescribe GSK products. A Chinese court fined GSK China a record 3 billion yuan (US$492 million) for bribery in 2014. The former head of GSK China and four other former GSK senior executives were also found guilty, and GSK China's financial compliance and legal departments were found to have been complicit. Related international investigations have been carried out in the United States by the DOJ and the Securities Exchange Commission (SEC) for potential violations of the Foreign Corrupt Practices Act, and in the United Kingdom by the SFO for possible breaches of the Bribery Act. The US investigation ended in a settlement in October 2016, with GSK paying the US SEC a US$20 million civil fine. The US DOJ and the SFO later declined to prosecute.

Privilege and data privacy: complexities in the Asia-Pacific region

With a mixture of common law and civil law jurisdictions, law enforcement agencies and regulators in the region adopt very different approaches to legal professional privilege

© Law Business Research 2021

and data protection. For example, China, Japan, Korea, Indonesia, Thailand and Vietnam do not recognise legal privilege, but lawyers owe duties of confidentiality over documents provided to them by their clients. However, this can be overridden by authorities in investigations.

In contrast, common law jurisdictions such as Hong Kong, Singapore, Malaysia, India, Australia and New Zealand all recognise legal privilege to a greater or lesser extent. In general, internal investigation notes and investigation reports produced in the context of corporate investigations may be covered by legal privilege and protected from disclosure in common law jurisdictions, depending on the extent of involvement of either internal or external lawyers in the investigation process. In the same vein, there is a basis for pushing back against seizure of privileged material during dawn raids or other inspections by authorities and regulators. This does not apply in civil law jurisdictions, meaning that in cross-border investigations, the approach of authorities and regulators on the question of legal privilege can be diametrically opposed. Corporates and their lawyers will often try to assert legal privilege in civil law jurisdictions, expecting it to be claimed as part of a broader regional investigation in which common law jurisdictions are also involved. However, this will not prevent documents and data being seized or handed over to authorities and regulators in civil law jurisdictions. These bodies could potentially then share the evidence with authorities and regulators overseas, resulting in a broader loss of privilege protection.

A related issue is data privacy. In the context of cross-border investigations, the extent to which Asian countries restrict data transfers offshore varies. India, for example, is in the process of introducing a Bill that, if passed, will introduce comprehensive protections for personal data modelled on the European Union's General Data Protection Regulation (GDPR). However, the draft law also includes data localisation provisions that require 'sensitive' and 'critical' personal data to be stored onshore. New Zealand has also passed amendments to its Privacy Act, which came into force in December 2020. The changes will bolster New Zealand's data privacy regime by, for example, introducing mandatory data breach reporting and restrictions on offshore transfers. However, China and Korea have already imposed very strict data protection requirements in the past few years, and China is continuing to build restrictions under its cybersecurity and data security laws. State secrets laws are usually also engaged in China, preventing the transfer offshore of documents that may contain politically sensitive information. However, more recently, China published a new draft Data Security Law for consultation, which provides significant additional restrictions and requirements, including a prohibition on providing data stored within China to foreign law enforcement authorities, without the prior approval of the Chinese authorities. In practice, most multinational companies in the region tend to seek employee consent for data use and transfer at the onboarding stage. However, these may not suffice under local laws, which should always be checked. For example, the prohibition contained in the draft Data Security Law in China will apply regardless of consent provided by a data subject and, in any event, applies to data more generally (i.e., not to personal data in particular). Personal data will be protected by another law, namely the proposed Personal Information Protection Law.

The extraterritorial nature of the GDPR adds a further potential layer of complexity for corporates operating in the Asia-Pacific region, since many have branches or processing operations within the European Union. The substantial fines that may be issued under

© Law Business Research 2021

the GDPR are a sober warning to all companies, regardless of location. Ensuring that the processing of data complies with the GDPR, where it applies, is a commercial imperative. In the context of investigations, the GDPR, in line with most domestic data privacy laws, gives authorities the right to receive personal data from investigated companies, or other authorities, in the context of regulatory criminal investigations. In internal investigations, a combination of processing conditions under the GDPR and local data privacy law exemptions and derogations (where applicable) will dictate whether transfers are permissible. This needs to be assessed in each individual case and will remain an area of interest in investigations in the region.

Increased pressure and incentives to co-operate

The Asia-Pacific region has seen the emergence of corporate settlement regimes in recent years. As seen in the United States and the United Kingdom, DPA regimes create strong incentives for self-disclosure by companies, and those that disclose, co-operate and remediate may avoid prosecution in favour of fines or monitorship. However, they have also been criticised as providing an ability to companies to 'buy' their way out of 'meaningful punishment'. This criticism has been directed at the Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019 by Australian Labor Party senators after it was reintroduced to the Senate at the end of 2019. The Australian Law Reform Commission has recently recommended some changes to the proposed regime to provide for judicial oversight.

These voluntary self-reporting regimes are to be differentiated from statutory reporting obligations that exist under many anti-money laundering laws across the region and in some jurisdictions in relation to certain predicate offences. Anti-money laundering laws may require the reporting of a suspicion of criminal proceeds flowing from a criminal act such as bribery. Laws in Malaysia and Vietnam go further and require the reporting of a bribery offence (regardless of whether the offence has resulted in criminal proceeds). The failure to report will often constitute a criminal offence in itself, and reporting obligations will need to be kept in mind whenever potential criminal misconduct is being investigated.

In anticipation of a new DPA regime in Australia, various authorities, including the Federal Police, have issued self-reporting guidelines to assist corporations that wish to self-report actual or suspected foreign bribery offences. Self-reporting (and co-operation) will be taken into account both in deciding whether to prosecute and, if prosecuted, as a mitigating factor during sentencing. Early guilty pleas by a company may also result in significant reductions in sentencing. New Zealand's regime falls short of a DPA system, but certain agencies, such as the Financial Markets Authority, may obtain 'enforceable undertakings' that help companies avoid prosecution.

Financial regulators such as the Securities and Futures Commission in Hong Kong, in limited circumstances, entertain negotiation resulting in reduced sanctions or declinations to prosecute. India and China have no non-prosecution agreement or DPA system, although in practice, self-reporting and co-operation may be taken into account in mitigation.

DPAs were introduced in Singapore in late 2018. This followed on the heels of the first multi-jurisdictional DPA entered into with the US DOJ involving Singaporean authorities. This was a rare example of a Singapore company being penalised by the Singapore

© Law Business Research 2021

authorities under national anti-bribery laws for bribery committed abroad. It was by far the highest penalty levied against a Singapore company and was the first DPA involving co-operation between the Brazil, Singapore and US authorities. Singapore's DPA regime is similar to that of the United Kingdom, except that Singapore DPAs cover a more limited range of criminal offences and Singapore prosecutors are not required to issue guidelines on when a DPA is appropriate and on what 'discounts' may be offered in the case of self-reporting, meaning that prosecutors retain maximum flexibility. Further, the Singapore DPA regime is unusual in that, unlike other jurisdictions with a DPA regime, Singapore has not yet introduced a corporate bribery offence, which means that there is likely to be less of an incentive to self-report and seek a DPA.

In Japan, a plea bargaining regime was introduced in June 2018. Unlike DPAs, this regime applies to individuals rather than companies. Suspects and defendants will be rewarded with leniency if they co-operate by providing information or evidence in resolving another person's crimes or by giving depositions against partners in crime (including corporates). This is likely to lead to an uptick in corporate investigations, as individuals become incentivised to inform the authorities about the activities of others, including their employers.

Whistleblowing regimes are a corollary of DPAs; both encourage early notification and co-operation. Australia has introduced new whistleblower protection laws, which came into effect on 1 July 2019. These strengthen protection and compensation for whistleblowers and impose on regulated companies the requirement to implement corporate whistleblowing frameworks, including confidentiality and non-retaliation provisions. India passed a Whistleblowing Act in 2014 but it has not yet been brought into effect. Long-awaited amendments were introduced to Japan's whistleblowing law in June 2020 to address criticism that its current law had no teeth, owing to the lack of sanctions on companies that treat whistleblowers unfairly. Although the amendments introduce additional protective elements, such as a duty to protect confidentiality, extend the scope of the law to former employees and provide for a duty to establish a reporting mechanism, there is still no provision for penalising companies that retaliate against a whistleblowing employee. Hong Kong and Singapore still lack dedicated whistleblower legislation, but do have provisions in a patchwork of laws and regulatory requirements to protect whistleblowers in certain circumstances. China's whistleblower legislation goes further than most in the region in including a reward mechanism for whistleblowers who report crimes to people's procuratorates. Various other financial reward schemes are scattered in sector-specific regulations. However, this does not compare to the huge financial incentives and bounties available in the United States under the Dodd-Frank Act. Regardless of incentives and protections, in Asia at least, there remain cultural and hierarchical norms that often militate against blowing the whistle and reporting up. These may mean that new legislation has limited traction, but time will tell.

© Law Business Research 2021

2

Europe Overview

Robert Dalling, Kelly Hagedorn and Matthew Worby[1]

Introduction

The European investigations landscape is characterised by a patchwork of varying legislative and regulatory frameworks and enforcement approaches. These are often shaped by past events and current political priorities in particular jurisdictions. These variations and the pace of change mean that cross-border investigations, whether involving multiple European jurisdictions or parallel investigations by enforcement authorities in other regions (or sometimes both), frequently present thorny practical and tactical challenges.

This overview does not seek to duplicate the commentary and analysis set out in many of the chapters in this volume. Rather, it looks at some of the key priorities of European enforcement authorities, focusing on anti-bribery and corruption, anti-money laundering, tax evasion and data protection. There is significant ongoing activity in these areas, and some authorities are adapting their approaches to make effective use of changes in the law and additions to their toolkits. This overview also looks ahead to seek to identify the key issues and trends on which those who are subject to investigations throughout Europe should be focusing.

Areas of enforcement risk

Anti-bribery and corruption

A substantial number of investigations by enforcement authorities have arisen following significant legislative developments that introduced corporate offences of failure to prevent bribery with extraterritorial effect (such as the UK Bribery Act 2010 (UKBA) and France's Sapin II Law). These legislative developments have been accompanied by new mechanisms enabling criminal investigations that involve corporate organisations

1 Robert Dalling and Kelly Hagedorn are partners and Matthew Worby is an associate at Jenner & Block London LLP.

© Law Business Research 2021

to be concluded through negotiated settlements. To date in Europe, these mechanisms have been used mainly (although not exclusively) in cases concerning historic bribery and corruption involving corporate organisations.

Following these developments, and despite a slow start, there has been increasing pressure for corporate criminal liability to be expanded to encompass other financial offences. The UK government, for example, commissioned a consultation in 2021 on the extent to which corporate criminal liability should be further reformed in England and Wales.[2]

Several other jurisdictions have introduced anti-bribery legislation in recent years, some of which has been the subject of criticism. In Ireland, for example, an offence analogous to the UK corporate offence of failure to prevent bribery came into force in July 2018.[3] However, the Irish statute has been described as flawed for failing to meet guidelines published by the Organisation for Economic Co-operation and Development (OECD). This is because the Irish statute requires dual criminality for an offence to be committed overseas.[4] Further, there is no guidance akin to that published by the UK Ministry of Justice in relation to 'adequate procedures' under the UKBA. There is therefore some remaining uncertainty among corporate organisations and their advisers as to exactly what 'taken all reasonable steps and exercised all due diligence' means in the Irish legislation, and how to avail oneself of a defence to the corporate offence. Given the nature of the Irish economy, and in particular its attractiveness to multinational technology and financial services companies, there is potential for investigations in Ireland to have significant cross-border elements, and clarity on this point would be welcome.

Elsewhere, German criminal law does not currently recognise the concept of corporate criminal liability. Although the German government introduced draft legislation in this area in August 2019, the legislation was not passed before the end of the same legislative session. As a result, the German government will need to reintroduce the draft legislation after the federal elections in September 2021 if it is to become law. It is unclear whether there is any appetite to do so.[5] In Poland, the OECD has described delays to legislation amending liability under Polish law for legal persons, and increasing financial penalties against corporations, as 'a serious concern'. It unclear whether the Polish government will enact any reform.[6]

2 https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/.

3 Ireland: Criminal Justice (Corporate Offences) Act 2018.

4 'Irish corruption law not in compliance with OECD guidelines', *The Irish Times* (26 August 2019), at https://www.irishtimes.com/news/crime-and-law/irish-corruption-law-not-in-compliance-with-oecd-guidelines-1.3997012.

5 'German corporate criminal liability reforms left in limbo', *Global Investigations Review* (2 July 2021), at https://globalinvestigationsreview.com/anti-corruption/german-corporate-criminal-liability-reforms-left-in-limbo.

6 'Poland's lack of progress in implementing reforms to boost fight against foreign bribery remains a serious concern' (22 June 2021), at https://www.oecd.org/poland/poland-s-lack-of-progress-in-implementing-reforms-to-boost-fight-against-foreign-bribery-remains-a-serious-concern.htm.

© Law Business Research 2021

Anti-money laundering

Although anti-money laundering (AML) enforcement remains high on most enforcement authorities' agenda, approaches to, and the resources available for, investigations vary considerably between European jurisdictions. This is despite the introduction of various iterations of the EU Money Laundering Directives (MLDs), which aim to standardise this area of enforcement. The latest MLD was the sixth, which EU Member States were due to implement by 3 December 2020. The sixth MLD seeks to regularise further the AML enforcement landscape in Europe, for example by:

- standardising the 22 predicate offences that must be considered 'criminal activity' for the purposes of money laundering by EU Member States;
- requiring EU Member States to expand criminal liability for money laundering to legal persons; and
- setting certain increased EU-wide minimum penalties for money laundering.

Although the effect of the sixth MLD is yet to be fully felt, enforcement action across Europe has continued apace. Some of the highest penalties imposed in recent years have resulted from investigations by Sweden's Financial Supervisory Authority[7] and the Netherlands' Public Prosecution Service.[8] These fines were issued for breaches of regulatory requirements and criminal law by major institutions in relation to their AML systems and controls. This marks a change, since France and the United Kingdom have historically imposed the heaviest fines in the region for AML-related transgressions. That is not to say that France's AML-related enforcement has not remained effective. The Autorité de Contrôle Prudentiel et de Résolution has reportedly focused in 2020 on smaller financial institutions, including payment service providers, rather than larger banks and money services businesses.

Fines are not the only notable feature of enforcement activity in this area. First, reflecting an increasingly close focus on individual accountability, regulators are now ready and able to pursue individuals considered to have played a part in AML failings. Second, it would appear that some European regulators are starting to initiate criminal prosecutions for this conduct at a corporate level. In 2021, the UK Financial Conduct Authority (FCA), for example, initiated its first criminal prosecution of a major financial institution for allegedly failing to prevent money laundering. It remains to be seen whether this prosecution will be successful, and the extent to which non-monetary penalties, such as reputational damage, will influence the approach of financial institutions in the future.

Tax evasion

Tax evasion is also increasingly attracting authorities' attention. In particular, several jurisdictions are seeking to prosecute a trading activity, known as cum-ex trading, whereby banks and stockbrokers engage in trading shares in a manner that allows both sides of a transaction to claim a tax rebate on the dividends purportedly paid by the shares.

7 Sweden: Swedbank was fined US$386 million for compliance deficiencies relating to Baltic money laundering, and Skandinaviska Enskilda Banken was fined €95 million for similar conduct.

8 Netherlands: ING Groep was fined US$900 million for broad failures relating to financial crime compliance controls.

© Law Business Research 2021

Germany is the most prominent example, where an estimated €31.8 billion was fraudulently claimed from the government in the form of rebates between 2001 and 2016.[9] It has been estimated that the total cost to the European taxpayer is more than €55 billion between 2001 and 2012.[10]

Enforcement action in response to such long-standing and wide-ranging conduct is complex, but has enjoyed some success. The Danish tax authority (SKAT), for example, charged three UK nationals and three US nationals for their role in allegedly defrauding the Danish treasury.[11] At least one former executive of a private bank in Germany has been sentenced to five and a half years for similar conduct, and two British nationals received suspended sentences in Germany.[12] However, enforcement action in response to this activity has not been entirely successful. Denmark, for example, is currently seeking to appeal a UK High Court decision ruling that SKAT cannot pursue a lawsuit seeking to recover £1.5 billion in the English courts.

More generally, the impact of fraud on the support measures introduced by various governments in response to the coronavirus pandemic has been well publicised. The UK government has announced an investment of £100 million in a Taxpayer Protection Taskforce to recover funds paid out incorrectly or as a result of fraud during the pandemic.[13] We anticipate other European jurisdictions will take a similar approach.

Data protection

The General Data Protection Regulation (GDPR) is now three years old and several themes are emerging. Following Brexit, we are yet to see any substantive divergence by the United Kingdom away from the GDPR, probably because of the UK's need to obtain an adequacy decision in respect of its data protection legislation, which it duly received in June 2021. Now that this decision has been obtained, potential divergence by the United Kingdom is a trend to watch for in 2022, as the UK government starts to consider how best to approach the digital economy and data protection outside the European Union.

The most significant trend we have seen thus far is the willingness of European data protection authorities to enforce the GDPR aggressively. A total of 880 fines have been

9 'Cum-ex tax scandal cost European treasuries €55 billion', DW Akademie (18 October 2018), at https://www.dw.com/en/cum-ex-tax-scandal-cost-european-treasuries-55-billion/a-45935370.

10 The Cum-ex files (information document), European Parliament, at https://www.europarl.europa.eu/cmsdata/158435/2018-11-26%20-%20Information%20paper%20on%20Cum-ex%20-%20Cum-cum.pdf.

11 'Dividend Reclaim Case: Six persons formally charged with defrauding the Danish Treasury of more than DKK 1 billion', Anklagemyndigheden, at https://anklagemyndigheden.dk/sites/default/files/inline-files/2096_PM_Udbyttesagen_North%20Channel%20Bank_EN.pdf.

12 'Banker first to be jailed in German tax fraud scandal', Reuters (1 June 2021), at https://www.reuters.com/legal/transactional/banker-first-be-jailed-german-tax-fraud-scandal-2021-06-01/.

13 'COVID-19: how HMRC will continue to support customers and the economy', HM Revenue and Customs, at https://www.gov.uk/government/publications/hmrc-issue-briefing-how-hmrc-will-continue-to-support-customers-and-the-economy/covid-19-how-hmrc-will-continue-to-support-customers-and-the-economy.

© Law Business Research 2021

issued, or declared, for a cumulative total of €1,291,357,143.[14] The largest fines have also been significant. Amazon may be fined up to €746 million by Luxembourg's data protection authority (at the time of writing the fine had been issued but was still subject to challenge by Amazon), and Google Inc was fined €50 million by the French data protection authority in 2019.

A developing trend of note is the role that non-governmental organisations have played in initiating data protection enforcement actions in the European Union. For example, La Quadrature du Net and None of Your Business (NOYB), French and Austrian pressure groups respectively, have reportedly filed (either collectively or individually) complaints that prompted the enforcement actions against Amazon and Google mentioned above. In addition to filing complaints, pressure groups are also litigating data protection issues directly. NOYB, through its leader Max Schrems, conducted the litigation that resulted in the US–EU Privacy Shield being declared invalid, and the Dutch pressure group Privacy Collective is reportedly suing Salesforce and Oracle in a class action targeting the cookie-tracking practices deployed by both companies. Corporates should therefore be aware that oversight of their data protection practices may be undertaken by civil society, not just regulators, and that those grievances may be taken to court.

Beyond the increasing importance of data protection as a risk area for corporates, investigators must now also keep data protection issues in mind when tackling a cross-border investigation. In particular, issues arising from the international transfer of personal data are becoming increasingly difficult globally, not just in Europe.

Increased pressure and incentives to co-operate

In England and Wales, the body of cases in which deferred prosecution agreements (DPAs) have been concluded between the Serious Fraud Office (SFO) and co-operating corporate organisations is slowly growing. Although the figure of 20 agreements per year predicted during the passage of the legislation that introduced DPAs seems unlikely to be achieved in the near term, the SFO entered into three DPAs in 2020 and three in 2021 (so far). This is the highest annual total for the SFO since the introduction of DPAs in the United Kingdom. Despite this increase, the SFO has itself been under pressure, having failed to date to secure the conviction of any individual named as an alleged offender in any of the DPAs. Against this backdrop, it remains to be seen whether the UK DPA regime will be considered a success, and if corporates will consider co-operation to be worthwhile. The SFO may also find itself under increasing scrutiny after it was revealed that the agency's enforcement activity has been markedly reduced during the coronavirus pandemic.

In France, the authorities responsible for investigating and prosecuting financial crime, the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF), have now concluded 13 published judicial public interest agreements (CJIPs)[15] with companies of various sizes, including one in which the global penalties imposed exceeded US$3.9 billion. A recent example also indicates that co-operation with

14 As at 4 October 2021. This figure includes notices of an intention to fine and so may be subject to change – see https://www.privacyaffairs.com/gdpr-fines/.

15 https://www.agence-francaise-anticorruption.gouv.fr/fr/convention-judiciaire-dinteret-public.

© Law Business Research 2021

the French authorities can result in a significant reduction in penalty. Systra, a transport company, saw its theoretical potential fine of €187 million ultimately levied at €7.5 million after the French authorities viewed the comprehensive compliance programme, in conjunction with historic offending, favourably.[16]

It remains to be seen whether further jurisdictions will enact similar measures. A November 2020 report published by the Irish government as part of measures to enhance Ireland's ability to fight economic crime declined to recommend the introduction of a deferred prosecution regime. In their report, the authors stated that they were 'not convinced that the introduction of a DPA regime will yield any significant benefit given the UK experience so far'.[17]

Although mechanisms similar to DPAs and CJIPs (or aspects of them) exist in some other jurisdictions around Europe, including Belgium, the Czech Republic, Romania and Slovakia, they are available only in some of these jurisdictions to resolve allegations of corruption, and the practice and procedure around the use of those mechanisms is not always clearly set out. It is also unclear whether any of these jurisdictions wish to expand these mechanisms. Concluded cases of the same magnitude as those seen in the United Kingdom and France have yet to be publicised.

The different approaches of European jurisdictions should be considered when dealing with global settlements. The Dutch company VEON, for example, entered into a joint global settlement with Dutch and US authorities to resolve an enforcement action under the US Foreign Corrupt Practices Act (FCPA), whereas Ericsson became the subject of an investigation by the Swedish authorities shortly after reaching a settlement to resolve an FCPA action with the US authorities.

In jurisdictions where DPAs are already established, authorities' and courts' expectations of co-operating corporate organisations in order for (1) negotiations to take place and (2) a settlement to be agreed and approved, are becoming clearer. In particular, the AFA and the PNF in France, and the SFO in the United Kingdom (in June and August 2019, respectively) have released guidance that clarifies their views on the co-operation needed to create the right conditions for a negotiated settlement to follow.[18] Courts and prosecutors have also provided guidance on whether corporate organisations are demonstrating the required levels of co-operation, while maintaining claims to legal professional privilege (where it is available).

16 'Regular compliance renewal helps French transport company minimise corruption fine', Global Investigations Review (2 August 2021), at https://globalinvestigationsreview.com/anti-corruption/regular-compliance-renewal-helps-french-transport-company-minimise-corruption-fine.

17 Department of Justice, 'Review Group Report on structures and strategies to prevent, investigate and penalise economic crime and corruption' (June 2021), at https://www.gov.ie/en/publication/be30e-review-group-report-on-structures-and-strategies-to-prevent-investigate-and-penalise-economic-crime-and-corruption/.

18 UK: see Serious Fraud Office, Corporate Co-operation Guidance, at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/>. France: see French Anti-Corruption Agency, at https://www.agence-francaise-anticorruption.gouv.fr/files/files/Lignes%20directrices%20PNF%20CJIP.pdf; https://www.agence-francaise-anticorruption.gouv.fr/fr/lafa-et-parquet-national-financier-precisent-mise-en-oeuvre-convention-judiciaire-dinteret-public.

© Law Business Research 2021

Culture and individual accountability

Among the most prominent themes in investigations concerning corporate organisations is the focus on culture, both at the time when alleged misconduct occurred and when any investigation is commenced. The definition of what constitutes 'good culture' is elusive. Authorities deciding whether to commence, continue and discontinue investigations (and selecting which charges to pursue) attach substantial importance to whether they consider alleged conduct (including individuals' conduct outside the workplace) to be indicative of a poor culture.

Although the FCA has historically published information about culture and governance as categories of enforcement data in their own right, it no longer does so. This perhaps suggests that the FCA views culture as pervasive across the firms that it regulates, and so it no longer needs to be explicitly identified as a stand-alone category.

The UK Senior Managers Certification Regime (SMCR) goes further than previous regulatory initiatives directed towards individual accountability. It gives the FCA and the Prudential Regulation Authority (PRA) powers to take action against a much broader population of individuals within firms. It also requires firms to document the specific responsibilities of their most senior executives, thus providing the FCA and PRA with clear road maps that may be used to hold those individuals accountable for breaches of regulatory requirements by firms. The FCA is now routinely using the SMCR for this purpose during enforcement investigations. Although enforcement authorities around Europe have been watching to see how the FCA and PRA seek to use these mechanisms to drive up standards of behaviour within the financial services industry, it remains to be seen whether other European regulators will follow the SMCR approach. By contrast, other common law jurisdictions, such as Singapore, Hong Kong and Australia,[19] have enacted regimes similar to the SMCR in recent years.

Even in countries where enforcement authorities have not explicitly named culture as an enforcement priority, boards are increasingly concerned to demonstrate their commitment to culture. Cases across Europe have shown the substantial reputational damage that can result from allegations of poor cultural practices and the speed at which allegations can cross borders (including into jurisdictions where enforcement authorities are active in this area).

Information sharing and multi-jurisdictional investigations

European investigation and enforcement authorities continue to collaborate actively with one another and with their counterparts globally, using mutual legal assistance treaties and other informal arrangements. There have been particularly noticeable increases in efforts to collaborate across borders where authorities have acquired the ability to enter into global settlements involving overseas enforcement authorities, and in GDPR-related enforcement.

Across Europe, traditional boundaries between enforcement authorities' remits are becoming increasingly blurred. The authorities are having to take an increasingly flexible

19 Singapore: Individual Accountability and Conduct Regime. Hong Kong: Manager-in-Charge Regime. Australia: Banking Executive Accountability Regime.

© Law Business Research 2021

view of what they are responsible for investigating, which authority should take the lead and how they should most effectively collaborate. Overlaps between the remits of antitrust, data protection and financial services enforcement authorities are becoming increasingly apparent. One example of this flexibility was the close co-operation between Luxembourg's and France's data protection authorities when Amazon was investigated for violating the GDPR.[20]

Enforcement authorities, conscious of the potential for duplication and delay, are anticipating these overlaps, both within and between jurisdictions, and are implementing mechanisms to facilitate collaboration. For example, following Brexit, the FCA entered into a series of detailed memoranda of understanding with the relevant national competent authorities within the European Union and the European Economic Area, setting out how these agencies will co-operate and exchange information.[21] Although convictions and other enforcement outcomes in one jurisdiction will commonly be the product of extensive information sharing between authorities, there are as yet few significant concluded examples of enforcement authorities simultaneously pursuing enforcement cases against the same targets in multiple European jurisdictions.

EU institutions as enforcement authorities

Historically, there have been relatively few examples of supranational European authorities (other than the European Commission (EC) in its role as an antitrust enforcement authority) taking overarching enforcement action. That said, there is a clear movement to facilitate greater co-operation and coordination with respect to enforcement activity at a European level. This is both as a response to past incidents in which regulatory arrangements were found to have been lacking and in an effort to counter perceived growing threats.

In particular, the European Union has stepped up its focus on a pan-European approach to AML enforcement following AML failings in various European states. Until now, AML legislation encouraging closer collaboration between national investigation and enforcement authorities has taken the form of successive AML Directives (which, as they are not directly effective instruments and require transposition by Member States into their national laws, have been implemented in different ways and to different extents). For example as of May 2021:

- only 70 per cent of EU Member States had been identified as having fully transposed the fifth MLD into their national laws, despite a deadline of January 2020;[22] and

20 'The Luxembourg data protection authority fined Amazon Europe Core €746 million', National Commission for Computing and Liberty (3 August 2021), at https://www.cnil.fr/fr/lautorite-luxembourgeoise-de-protection-des-donnees-prononce-lencontre-damazon-europe-core-une.

21 'MoUs with European authorities in the areas of securities, investment services and asset management, insurance and pensions, and banking', Financial Conduct Authority (4 January 2021), at https://www.fca.org.uk/news/statements/mous-european-authorities-securities-insurance-pensions-banking.

22 'Anti-money laundering directive V (AMLD V) – transposition status', European Commission (2 June 2020), at https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en.

© Law Business Research 2021

- the fourth MLD had yet to be completely transposed into the national laws of all EU Member States, despite 16 June 2017 being the deadline for doing so.[23]

The European Banking Authority (EBA) was given additional powers following several well-publicised AML failings. As of 1 January 2020, the EBA has been:

- tasked with coordinating national authorities' supervisory responsibilities in respect of AML activity;
- empowered to lead on the establishment of AML policies by national authorities; and
- required to monitor the implementation of AML standards within Europe.[24]

An example of the EBA's work in this area can be found in the revised guidelines on money laundering and terrorist financing risk factors published in March 2021. As part of a general update to the AML landscape in the European Union (EU AML), the guidelines address new money laundering risk factors and seek to develop more effective and consistent supervisory approaches across Europe.[25] It is apparent that the EBA will continue to rationalise the AML landscape. On 2 August 2021, the authority published a consultation paper[26] seeking views on draft guidelines setting out the role, tasks and responsibilities of AML compliance officers under the fourth MLD. It is the first time that the regulatory expectations for AML compliance officers have been set out at a European level, apparently with a view to adopting a similar EU-wide approach such as that required under the GDPR for data protection officers.

Despite this activity, arrangements are still far from uniform across Europe. The extent to which the requirements set out in successive MLDs have been effectively transposed, and other provisions relating to cross-border collaboration and resourcing of national authorities have been implemented, varies widely between jurisdictions and will require further action to resolve.

In some instances, bilateral and multinational arrangements are in place, helping authorities to deploy their resources as effectively and efficiently as possible in cross-border AML investigations. The most recent example, which is also a response to the concerns about previous enforcement arrangements already mentioned, is a formal mechanism to enable Baltic and Nordic AML regulators to exchange information and coordinate

23 'Anti-money laundering directive IV (AMLD IV) – transposition status', European Commission (5 October 2020), at https://ec.europa.eu/info/publications/anti-money-laundering-directive-4-transposition-status_en.

24 Regulation (EU) 2019/2175.

25 'EBA publishes final revised Guidelines on money laundering and terrorist financing risk factors', European Banking Authority [EBA] (1 March 2021), at https://www.eba.europa.eu/eba-publishes-final-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors.

26 Consultation Paper: Draft Guidelines: 'On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849', EBA, at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20draft%20Guidelines%20on%20the%20role%2C%20tasks%20and%20responsibilities%20AML-CFT%20compliance%20officers/1018277/CP%20GLs%20on%20AMLCFT%20compliance%20officer.pdf.

© Law Business Research 2021

enforcement action. There are also increasingly sophisticated mechanisms in place in some jurisdictions to enable information sharing between private sector organisations, and with enforcement authorities.[27] In July 2020, the Netherlands Bankers' Association announced that the country's three largest banks and two smaller lenders would create a purely private joint transaction monitoring body, called Transaction Monitoring Netherlands,[28] designed to flag activity of concern that would not necessarily be identified as suspicious by a single institution's compliance department. Transaction Monitoring Netherlands is due to begin monitoring transactions in 2021. However, at the time of writing, it was unclear whether it had.[29]

The EC also appears determined to take further action. On 20 July 2021, it unveiled a further package of legislative proposals to strengthen the EU AML framework. The package included the creation of a new EU enforcement agency tasked with combating money laundering, called the Anti-Money Laundering Authority (AMLA).[30] The intent is to establish AMLA as a 'centrepiece' of a supervisory system that includes national authorities. This will allow the EC to directly supervise certain high-risk entities and join the front-line of AML enforcement. This is a welcome development in light of recent AML scandals, which invariably involve a cross-border element, leaving national enforcement agencies piecing together an incomplete picture after the conduct has completed.

Away from AML enforcement, the EC remains active as an antitrust enforcement authority. Some long-standing themes continue to feature in European antitrust investigations. There are exceptions to rules relating to legal professional privilege (in jurisdictions where it is part of the legal landscape). Leniency provisions often do not dovetail neatly with other regulatory mandatory reporting obligations. There are significant variations in the approaches taken by the EC and national competition authorities. There would also appear to be a different focus on sectors of enforcement. The EC appears to be concentrating on technology companies, as opposed to perhaps the more traditional financial crime targets, namely financial institutions and extractive industries. These, and other themes, mean that European antitrust investigations have to be handled differently from those pursued by other regulators.

In other areas, authorities with a pan-European remit have been active. The European Anti-Fraud Office (known as OLAF), the division of the EC responsible for investigating fraud against the EU budget, and corruption and serious misconduct within EU institutions, has been particularly active in conducting investigations. The most recent available

27 In the United Kingdom, with effect from October 2017, previously voluntary arrangements enabling information sharing within the private sector and between private sector organisations and enforcement authorities were placed on a statutory footing – Criminal Finances Act 2017, s.11 (which amended the Proceeds of Crime Act 2002).

28 See press release, Netherlands Bankers' Association, 'Transaction Monitoring Netherlands: a unique step in the fight against money laundering and the financing of terrorism', at https://www.nvb.nl/english/transaction-monitoring-netherlands-a-unique-step-in-the-fight-against-money-laundering-and-the-financing-of-terrorism/.

29 See https://tmnl.nl/summary-eng/.

30 https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en.

© Law Business Research 2021

statistics indicate that OLAF concluded 230 investigations and commenced 290 investigations during 2020 and recommended that national authorities take action to recover nearly €294 million in 2020.[31]

In addition, Europol has conducted extensive work to seek to coordinate national responses and lay the foundations for possible future multilateral criminal enforcement action in a number of areas, including notably in relation to large-scale cyberattacks[32] and the coronavirus pandemic.[33]

It seems likely that levels of coordinated pan-European criminal enforcement action will increase in future. The new European Public Prosecutor's Office (EPPO) became operational in June 2021. In the 22 Member States that have signed up to the arrangements establishing it,[34] EPPO will have powers to investigate and prosecute crimes against the EU budget, such as fraud, corruption and tax fraud valued at over €10 million. It will not replace OLAF or other existing investigating and prosecuting authorities (or national enforcement authorities) but will pool experience, adopt a consistent prosecution policy, and be able to use streamlined procedures for the exchange of information across borders. Laura Codruța Kövesi, the current head of EPPO and European Chief Prosecutor, has indicated a willingness to use EPPO's powers extensively.[35] Indeed, following a lengthy preparatory phase, EPPO started its investigations promptly, organising a coordinated series of searches in early August 2021 across five European jurisdictions in connection with a VAT fraud estimated to be worth €14 million.[36]

Brexit certainty?

Despite fears that Brexit would cause significant damage to cross-border investigations and enforcement, the December 2020 trade and co-operation deal (the Brexit Deal) did much to limit the consequences of Brexit in the areas of enforcement and investigations. In the context of the Irish border (a potential enforcement flashpoint), a UK parliamentary committee found (in April 2021) that 'Brexit had had no discernible operational

31 See European Anti-Fraud Office, 'The OLAF Report 2020', at https://ec.europa.eu/anti-fraud/system/files/2021-09/olaf_report_2020_en_0.pdf, p. 3.

32 See press release, Europol (30 June 2021), at https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups.

33 See press release, Europol (22 June 2021), https://www.europol.europa.eu/newsroom/news/terrorists-attempted-to-take-advantage-of-pandemic-says-europol%E2%80%99s-new-eu-terrorism-situation-and-trend-report-2021.

34 Sweden, Hungary, Denmark, Ireland and Poland having opted out.

35 See further details in relation to the European Public Prosecutor's Office at https://europa.eu/rapid/press-release_MEMO-17-1551_en.htm, and the appointment of the European Chief Prosecutor at www.europarl.europa.eu/news/en/press-room/20190923IPR61749/kovesi-to-become-eu-chief-prosecutor.

36 'Premises in Germany, the Netherlands, Slovakia, Bulgaria and Hungary searched in the framework of an EPPO investigation into cross-border VAT fraud' (4 August 2021), at https://www.eppo.europa.eu/en/news/premises-germany-netherlands-slovakia-bulgaria-and-hungary-searched-framework-eppo.

© Law Business Research 2021

impact on cross-border policing and the ability to co-operate with partners in the EU has been maintained'.[37]

In addition to the Brexit Deal, the steps that the UK government took to maintain access to a similar level of information from European enforcement agencies following Brexit appear to be helping to maintain the status quo. In February 2021, the UK government stated that the Interpol systems and Warning Index used by the United Kingdom for law enforcement purposes, which are no longer automatically integrated into the UK Police National Computer following Brexit, update at broadly the same speed as the pre-Brexit systems.[38]

It should be noted, however, that Brexit is still only a recent development and that a greater impact may become apparent over time. It is likely that an assessment will only be possible once the backlog of pre-Brexit investigations and cases is resolved, and authorities begin to tackle post-Brexit investigations and cases. Areas of future concern include the European Investigation Order scheme and issues in replacing the European Arrest Warrant (EAW) scheme in the United Kingdom.

The United Kingdom is no longer part of the European Investigation Order scheme. The Brexit Deal provided that UK–EU arrangements would revert to a mutual legal assistance scheme governed by a 1959 convention. It would appear that the process of obtaining information under these new arrangements might take longer. Although the European Investigation Order scheme gave states 30 days from the receipt of a request to decide whether to execute it, the new arrangements allow 45 days.

Further, following its withdrawal from the EAW system, 10 EU Member States have notified the United Kingdom of their intention to exercise an absolute bar on the extradition of their own nationals to the United Kingdom, and an additional two nations shall only extradite their own nationals to the United Kingdom with the individual's consent.[39] It appears that the European and United Kingdom will need to take care to ensure cross-border enforcement action can be maintained, otherwise it is possible that the UK government will soon find it difficult to close cases against individuals of certain nationalities who have returned to their home nation in Europe. Before Brexit, the EAW would probably have resolved the issue. It remains to be seen whether this will prove to be a significant challenge for UK enforcement activity in the future.

37 'Cross-border co-operation on policing, security and criminal justice after Brexit', Northern Ireland Affairs Committee (22 April 2021), at https://committees.parliament.uk/publications/5650/documents/55754/default/.

38 National Crime Agency – Written evidence (PBS0001): Post EU Exit Law Enforcement Cooperation (3 February 2021), at https://committees.parliament.uk/writtenevidence/23533/pdf/.

39 Home Office – Written evidence (PBS0002): EU Member State Notifications under the Law Enforcement and Criminal Justice Title of the Trade and Cooperation Agreement, including Extradition Of Own Nationals (5 March 2021), at https://committees.parliament.uk/writtenevidence/23544/pdf/.

© Law Business Research 2021

3

Latin America Overview

María González Calvet[1]

Introduction

Combating corruption through unprecedented international coordination

One would be hard-pressed to find a region that has captured the attention of anti-corruption practitioners, academics, regulators, enforcement officials and international organisations such as the Organisation for Economic Co-operation and Development (OECD) and Transparency International more than Latin America has during the past decade. The increased attention was sparked principally by the *Lava Jato* (*Operation Car Wash*) scandal and its ensuing cross-border investigations that left virtually no country in the region untouched and sprawled across other jurisdictions around the globe. Numerous lessons emerged from *Operation Car Wash*, one of the most significant anti-corruption enforcement efforts in modern times. Of those, one stands out in particular: the transformative impact of effective international co-operation.

As a result of *Operation Car Wash* and coordination between authorities in multiple jurisdictions, Latin American authorities have cultivated a newfound appreciation of how to employ various international co-operation tools and mechanisms. The ability of prosecutors and investigators across the region to respond to transnational corruption scandals also results from their increased participation in multilateral initiatives. Inspired by these international efforts and encouraged by ever-evolving best practices and standards, practitioners in the region have conducted notable investigations by forging lasting partnerships with foreign counterparts and utilising previously ignored tools to exchange information and act on leads and evidence. These measures include making better use of financial intelligence obtained through specialist agencies and proactively forming dynamic anti-corruption law enforcement networks that allow authorities to communicate directly

1 María González Calvet is a partner at Ropes & Gray LLP. Other contributors to this chapter include Ropes & Gray associates Kent Ford and Stephanie Colorado.

© Law Business Research 2021

and exchange crucial evidence and information in real time. Furthermore, during the past decade, numerous countries in the region have enacted corporate liability frameworks to tackle large-scale wrongdoing by companies. These efforts have emboldened prosecutors and regulators and vested administrative enforcement bodies with the authority to share information more readily with foreign authorities when investigating corporate corruption. The fruits of this increased international co-operation are evidenced by the surge in prosecutions, assets recovered and individual convictions. In Brazil, for example, prosecutors have issued more than 1,450 search and seizure warrants[2] and secured nearly 280 convictions[3] in the *Operation Car Wash* scandal alone.

However, anti-corruption efforts in Latin America temporarily slowed in light of the covid-19 crisis and related public sector budget cuts, and it is unclear how quickly the anti-corruption momentum gained in the region prior to the crisis will resume as the pandemic subsides.[4] Nonetheless, the US Department of Justice (US DOJ) continued to pursue enforcement actions, and US Foreign Corrupt Practices Act (FCPA) resolutions reached jointly during the pandemic between US and local agencies in South America, together with the Biden administration's announced desire to collaborate with Latin American officials to address corruption, signal that efforts to fortify international co-operation and enforcement in the region will continue in the years to come.[5]

This chapter analyses the international co-operation instruments and mechanisms that exist across Latin American jurisdictions and discusses the evolution and efficacy of these frameworks. It also considers the origins of paradigm shifts in enforcement, and the successes and obstacles that anti-corruption authorities have encountered to date.

Mechanisms of international co-operation

Law enforcement authorities have several international co-operation tools at their disposal when conducting multi-jurisdictional corruption investigations. Countries in the region have increasingly supplemented bilateral co-operation activity with participation in multilateral efforts to root out corruption, including the OECD Anti-Bribery Convention, the Inter-American Convention Against Corruption (IACAC) and the

2 Gaspard Estrada, 'Operation Car Wash Was No Magic Bullet,' *The New York Times* (26 February 2021), at https://www.nytimes.com/2021/02/26/opinion/international-world/car-wash-operation-brazil-bolsonaro.html; Ministerio Publico Federal, Caso Lava Jato – Resultados (last updated 24 August 2021), at http://www.mpf.mp.br/grandes-casos/lava-jato/resultados.

3 Amelia Cheatham, 'Lava Jato: See How Far Brazil's Corruption Probe Reached', Council on Foreign Relations (19 April 2021), at https://www.cfr.org/in-brief/lava-jato-see-how-far-brazils-corruption-probe-reached.

4 'Status of Latin America's Anti-corruption Fight amid Health and Political Challenges', Congressional Research Services (21 April 2020), at https://sgp.fas.org/crs/row/IN11350.pdf; Geert Aalbers, 'Headwinds in the fight against corruption in Latin America', Control Risks (2021), at https://www.controlrisks.com/our-thinking/insights/headwinds-in-the-fight-against-corruption-in-latin-america.

5 Silva Avalos, 'Biden and Central America's Anti-Corruption Crusade', InSight Crime (15 February 2021), at https://insightcrime.org/news/will-biden-spearhead-creation-anti-corruption-commission-central-america/.

© Law Business Research 2021

United Nations Convention against Corruption (UNCAC).[6] These efforts have intensified the fight against corruption and encompass innovative, expansive and informal means of collaboration, leading to an increase in direct relationships, regular information sharing and stronger enforcement networks across Latin America.

Formal anti-corruption co-operation instruments

Historically, Latin American law enforcement authorities have sought and provided mutual legal assistance (MLA) in anti-corruption matters through formal legal channels made available by bilateral treaties and other similar instruments. Cross-jurisdictional efforts started as early as 1996 with the IACAC, which required Member States to co-operate in extradition efforts and provide mutual assistance to prosecute corruption.[7]

If used effectively, bilateral MLA treaties (MLATs) can be crucial to the success of multi-jurisdictional investigations. This is particularly so in the context of corruption crimes, which are often complex in nature and require sophisticated knowledge of illicit financial flows and transactions to detect and combat criminality proactively. MLA can be overly formal and time-consuming but it is often the best way to ensure that foreign evidence is admissible in domestic proceedings.

During the past two decades, Latin American jurisdictions have gradually constructed a network of formal agreements that enable their respective authorities to provide MLA. For example, Brazil has concluded bilateral MLATs with Colombia, Honduras, Mexico, Panama and Peru, and a number of jurisdictions outside Latin America.[8] Colombia has entered into MLATs with Argentina, Brazil, Cuba, Ecuador, Mexico, Panama, Paraguay, Peru and Venezuela, as well as some non-Latin American jurisdictions.[9] Additionally, the Member States of Mercosur (Argentina, Brazil, Paraguay, Uruguay, Bolivia and Chile) have signed a Protocol of Mutual Legal Assistance in Criminal Matters (also known as the Protocol of San Luis).[10] Despite the initially slow evolution of MLATs in the region,

---

6 'Strengthening Enforcement of the OECD Anti-Bribery Convention', Transparency International, at https://www.transparency.org/en/projects/strengthening-enforcement-of-the-oecd-anti-bribery-convention-1# (last accessed 6 August 2020) ('Despite some high-profile fines and prosecutions, our research shows that enforcement of foreign bribery laws among most OECD countries is shockingly low.').

7 Inter-American Convention Against Corruption (IACAC) (B-58), Articles XIII and XIV (29 March 1996), Organization of American States (OAS), at www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp.

8 Ministry of Justice and Public Security (Brazil), Bilateral Mutual Legal Assistance Agreements relating to Criminal Matters (in Portuguese), at https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais/acordos-bilaterais-1 (last accessed 24 August 2021).

9 Ministry of Justice (Colombia), Judicial Assistance (in Spanish), at https://www.minjusticia.gov.co/servicio-ciudadano/Documents/tramites-servicios/servicios/ASISTENCIA%20JUDICIAL.pdf (last accessed 1 September 2021).

10 European Commission, 'Study on judicial cooperation, mutual legal assistance and extradition of drug traffickers and other drug-related crime offenders, between the EU and its Member States and Latin American and Caribbean (LAC) countries', at 69 (2013), at https://op.europa.eu/en/publication-detail/-/publication/c7015d8f-2511-4909-99bf-d217602ee599.

© Law Business Research 2021

their use became essential from 2014 as anti-corruption enforcement action surged because of major international corruption scandals.[11]

The prosecution of several companies in connection with *Operation Car Wash* serves as a key example of MLATs working at their best. In 2017, the US DOJ, alongside the Brazilian *Operation Car Wash* taskforce (housed within Brazil's Federal Public Prosecutor's Office),[12] coordinated resolutions in four cases under the FCPA against Embraer, Rolls-Royce, Braskem and Odebrecht. In July 2017, the then Acting Assistant Attorney General for the Criminal Division of the US DOJ, Kenneth A Blanco, explained that by working together, 'Brazil and the Department not only assisted one another in gathering evidence and building the case, but made sure to credit the fines and penalties paid to each country, rather than imposing duplicative fines and penalties'.[13] As explained by Blanco, US and Brazilian authorities assisted one another in gathering information through direct informal communications. A prosecutor or financial intelligence unit (FIU) agent, for example, could call his foreign counterpart at the beginning of an investigation to identify bank accounts of interest. The prosecutors later sought formal MLA to request evidence so that it would be admissible at trial.[14] In the wake of *Operation Car Wash*, which formally concluded in early 2021,[15] prosecutors across the region have increasingly resorted to MLATs not only to obtain evidence located abroad but also – and perhaps even more importantly – to recover and repatriate millions in illicit assets and criminal proceeds concealed in overseas bank accounts.[16]

If two countries do not have an MLAT in place, their respective authorities may be able to provide co-operation and assistance pursuant to multilateral conventions and agreements allowing for coordination on matters relating to anti-corruption.

The IACAC, for example, targets specific corruption practices at the national level and aims to develop complex international anti-corruption regimes to facilitate cross-border co-operation.[17] Specifically, Article 14 of the IACAC provides that 'States Parties shall

11 'Combating Corruption in Latin America: Congressional Considerations', Congressional Research Services (21 May 2019), at https://fas.org/sgp/crs/row/R45733.pdf.

12 '"Car Wash" Probe Faces New Challenges', *Associated Press* (2 October 2019), at https://www.voanews.com/americas/car-wash-probe-faces-new-challenges.

13 US Department of Justice (US DOJ), press release, 'Acting Assistant Attorney General Kenneth A. Blanco Speaks at the Atlantic Council Inter-American Dialogue Event on Lessons From Brazil: Crisis, Corruption and Global Cooperation' (19 July 2017), at https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-atlantic-council-inter-american-1.

14 Id. The US–Brazil 1997 bilateral treaty, which lays the groundwork for developing mutual legal assistance (MLA), does not appear to prohibit informal communications pursuant to an investigation. See 'Mutual Legal Assistance Treaty Between the United States and Brazil' (14 October 1997, 80 Stat. 721), at https://www.state.gov/wp-content/uploads/2019/02/12889-Brazil-Law-Enforcement-MLAT-10.14.1997.pdf.

15 Ricardo Brito and Gram Slattery, 'After seven years, Brazil shuts down Car Wash anti-corruption squad', *Reuters* (3 February 2021), at https://www.reuters.com/article/us-brazil-corruption-idUSKBN2A4068.

16 Vladimir Aras, 'Effective Measures for Asset Recovery: The Brazilian Approach' (2017), at https://www.unafei.or.jp/publications/pdf/RS_No104/No104_17_VE_Aras_2.pdf.

17 Summit of the Americas, Plan of Action, No. 5, Miami, Florida, 11 December 1994, at www.summit-americas.org/miamiplan.htm#11.

© Law Business Research 2021

afford one another the *widest* measure of mutual assistance by processing requests from authorities that . . . have the power to investigate or prosecute the acts of corruption . . . and to obtain evidence and take other necessary action to facilitate legal proceedings and measures regarding the investigation or prosecution of acts of corruption'.[18] Notably, Argentina incorporated this language in its law on international co-operation in criminal matters.[19] The Mechanism for Follow-Up on the Implementation of the Inter-American Convention against Corruption, which oversees the monitoring of IACAC States Parties' implementation of the Convention, does not regularly provide statistics on the number of MLA requests countries have submitted pursuant to the instrument.

The ratification of the OECD Anti-Bribery Convention strengthened the global fight against corruption, particularly by pushing Member States to criminalise bribery of foreign public officials and to introduce corporate liability for foreign bribery.[20] The OECD Working Group on Bribery (WGB), a peer-led body composed of OECD Anti-Bribery Convention Member States, is charged with monitoring and evaluating implementation and enforcement of the Convention by Member States. All Member States undergo periodic formal peer review processes whereby their anti-corruption policies and their implementation and enforcement are evaluated by experts designated by peer Member States.[21] Each review culminates in a final report, which is made public.[22] Considered by Transparency International to be the 'gold standard' of monitoring, the WGB has brought transformational changes to Latin America's anti-corruption legislative and enforcement landscapes. In response to WGB reviews, nearly all Latin American Member States (Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico and Peru) have introduced some form of corporate liability for foreign bribery (four of which did so in the past five years).[23]

---

18 IACAC, Article XIV (emphasis added).

19 See 'Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-Step Guide 2012', G20 (2012), at https://www.bmjv.de/SharedDocs/Downloads/EN/G20/Requesting%20Mutual%20Legal%20Assistance%20in%20Criminal%20Matters%20from%20G20%20Countries%20-%20A%20step-by-step%20guide.pdf?__blob=publicationFile&v=1.

20 Senate Executive Report 106–15 (20 June 2000), at https://www.govinfo.gov/content/pkg/CRPT-106erpt15/html/CRPT-106erpt15.htm; Organisation for Economic Co-operation and Development (OECD) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, at www.oecd.org/corruption/oecdantibriberyconvention.htm (last accessed 27 August 2021).

21 'Country monitoring of the OECD Anti-Bribery Convention', OECD, at https://www.oecd.org/corruption/countrymonitoringoftheoecdanti-briberyconvention.htm (last accessed 14 August 2020); 'Phase 1 country monitoring of the OECD Anti-Bribery Convention', OECD, at https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/phase1countrymonitoringoftheoecdanti-briberyconvention.htm (last accessed 27 August 2021).

22 'Country monitoring of the OECD Anti-Bribery Convention' (footnote 21, above).

23 '2020 Latin America Corruption Survey', Miller & Chevalier (8 July 2020), at 20, at https://www.millerchevalier.com/sites/default/files/publications/LACS/2020-Latin-America-Corruption-Survey-Report_English.pdf.

© Law Business Research 2021

In addition to formal reviews, the WGB facilitates interdisciplinary multi-jurisdictional training programmes for enforcement authorities on investigative techniques.[24]

Finally, the UNCAC is the most comprehensive legally binding international anti-corruption treaty and has the most Member States. It covers both domestic and foreign bribery and promotes co-operation and information sharing, including MLA, extradition and bank secrecy.[25] Similar to the IACAC, Article 18 of the UNCAC provides that 'States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings' and includes many categories of assistance found in bilateral MLATs (e.g., taking evidence or statements from people, executing searches and seizures, and identifying and tracing proceeds of crime). Latin American jurisdictions without bilateral MLATs use the UNCAC as a legal basis for seeking and requesting assistance, which authorities execute pursuant to domestic law allowing for non-treaty-based MLA requests. In Brazil, for example, the UNCAC has facilitated MLA extradition requests in the absence of dual criminality, as the Convention allows for extradition even when the alleged violation of law is not defined in the same manner or under similar categories across all involved jurisdictions.[26]

Memoranda of understanding

Partly in response to the UNCAC's mandate for facilitating MLA, some Latin American countries are codifying their co-operation efforts through memoranda of understanding (MOUs). Owing to their ad hoc nature, MOUs streamline and simplify cross-border co-operation, allowing regulators to avoid lengthy and bureaucratic processes that often delay the process of MLA requests.[27] MOUs afford jurisdictions working with Latin American regulatory and administrative enforcement authorities an informal way of receiving assistance in the form of intelligence, procedural instructions or data collection prior to requesting MLA.[28] MOUs are also invaluable resources when working with jurisdictions that lack a comprehensive MLA framework.

In 2018, Colombia signed MOUs relating to international bribery with Argentina, Chile, El Salvador and Guatemala, and invited other countries, including Mexico, Costa

24 See, e.g., 'OECD Latin America Academy for Tax and Financial Crime Investigation', OECD, at https://www.oecd.org/tax/crime/latin-america-academy-for-tax-and-financial-crime-investigation.htm (last accessed 27 August 2021).

25 'The United Nations Convention Against Corruption: A Model Academic Course', United Nations Office on Drug and Crime (UNODC), at https://www.unodc.org/documents/corruption/Education/ACAD/UNCACModelCourse/UNCAC_Academic_Course_English.pdf (last accessed 12 August 2020).

26 'United Nations Convention Against Corruption', Liaison and Partnership Office in Brazil, UNODC, at https://www.unodc.org/lpo-brazil/en/corrupcao/convencao.html (last accessed 14 August 2020); 'Country Review Report of Brazil', 107, UNODC (19 January 2017), at https://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2017_01_19_Brazil_Final_Country_Report.pdf.

27 'Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions', ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, 33 (2017), at https://www.oecd.org/corruption/ADB-OECD-Mutual-Legal-Assistance-Corruption-2017.pdf.

28 Id.

© Law Business Research 2021

Rica, Ecuador, Honduras, Uruguay and Nicaragua, to negotiate MOUs.[29] In 2017, Colombia's Superintendency of Corporations, a regulatory body charged with investigating and sanctioning legal persons for acts of bribery, concluded an MOU with Peru for the purpose of investigating transnational corruption through bilateral exchanges of evidence in as close to real time as possible.[30] These types of agreements obviate the need for more formal MLA processes and enable regulators to gain access to the same types of information (in the form of documents, data and files) that they would be able to obtain while carrying out their own investigations domestically. As a result, MOUs have emerged as a tool in overcoming the difficulties of cross-border investigations and are further evidence of the ability of anti-corruption bodies in the region to adapt their activity to the evolving nature of transnational corruption.

Joint investigation teams

Joint investigation teams (JITs) allow law enforcement officials from multiple countries to carry out criminal investigations in multiple jurisdictions. Member States sign a formal agreement establishing the JIT's purpose, duration and composition. JITs include investigators, prosecutors and occasionally judges led by the jurisdiction in which the majority of the investigative measures will take place, with seconded law enforcement officials from other countries. As with MOUs, JITs allow for greater speed than the traditional MLA process, and have the added benefit of ensuring better coordination and quality of evidence as participating investigators from different countries work hand in hand. In 2019, for example, Argentina joined a JIT with Spain and Italy to investigate an organised criminal group operating in all three countries that was accused of distributing approximately two tons of cocaine.[31] The investigation began in November 2017 when authorities detained two individuals after discovering in their possession three suitcases containing €365,000.[32] In December 2018, Spanish and Argentinian authorities simultaneously raided 73 homes and detained 35 individuals.[33] The JIT was subsequently formed and the nations together identified members of the illicit organisation and approximately

29 Superintendency of Corporations, 'Strategic Planning Monitoring Fourth Quarter 2018' (31 December 2018) (in Spanish), at https://www.supersociedades.gov.co/nuestra_entidad/Contratacion/Documents/2018/4-Seguimiento-2018-trimestre-IV.pdf.

30 'Colombia y Perú contra soborno transnacional', *El Nuevo Siglo* (23 September 2017), at www.elnuevosiglo.com.co/articulos/09-2017-colombia-y-peru-combatiran-soborno-transnacional.

31 'Argentina: Follow-up To The Phase 3bis Report & Recommendations', OECD Working Group on Bribery, at 141 (July 2019), at https://www.oecd.org/corruption/anti-bribery/OECD-Argentina-3bis-follow-up-report-ENG.pdf; 'Major drugs bust leads to 48 arrests in Spain, Argentina and Italy', European Observatory of Crimes and Security (EU-OCS) (26 December 2018), at https://eu-ocs.com/major-drugs-bust-leads-to-48-arrests-in-spain-argentina-and-italy/.

32 'Piden juicio para el clan Loza por eniar drogas a España en 4x4 y pescados', *El Ciudadano* (12 October 2019), at https://www.elciudadanoweb.com/piden-juicio-para-el-clan-loza-por-enviar-drogas-a-espana-en-4x4-y-pescados/.

33 'Equipos Conjuntos de Investigacion: Estrategias de trabajo articulado para investigar y perseguir al crimen organizado', Ministerio Publico Fiscal de Argentina (2019), at 12, at https://www.fiscales.gob.ar/wp-content/uploads/2019/12/DGCRI_Equipos-Conjuntos_2019.pdf.

© Law Business Research 2021

US$15 million of laundered money. The JIT's investigation involved the co-operation of more than 750 police officers across three countries.[34] On 23 December 2019, the Federal Oral Tribunal of Salta convicted several members of the criminal organisation of transporting and storing narcotics.[35]

JITs are still a novel concept in Latin American countries and only time will tell if the region's anti-corruption authorities will fully appreciate their potential benefits. Nevertheless, international and national bodies have continued to press for their increased use in the region. The European Union has been particularly influential in this regard; its EL PAcCTO programme has been behind five of the 10 JITs formed in Latin America in recent years.[36]

Financial intelligence exchanges

The crime of corruption goes hand in hand with money laundering and other types of financial wrongdoing. For this reason, bodies such as national FIUs are essential for detecting money laundering activity and the predicate offence of bribery. FIUs are in a unique position to analyse, package and share complex financial information not only domestically, but also with their foreign counterparts.

Latin American FIUs have become more active in fighting corruption. The intergovernment anti-money laundering organisation known as Financial Action Task Force has noted increases in requests and information exchanges between Latin American FIUs through various mechanisms, including the Egmont Group Secure Web and MOUs. Notably, in 2014, the FIUs of Peru, Chile, Colombia and Mexico created a co-operation framework, allowing them, among other things, to exchange information on cross-border transportation of currency, strategic analysis and money laundering convictions – all valuable tools for detecting and preventing corruption.[37] Between 2014 and 2018, Peru's FIU issued 515 foreign information requests to more than 30 countries, of which 76 were issued to Mexico, Chile and Colombia.[38] Further, Mexico's FIU plays an important part in anti-corruption enforcement by freezing bank accounts and providing information to prosecutors.[39] In May 2019, account-freezing proved effective in corruption investigations against the former head of Mexico's national oil company, Pemex, and the chairman

34 'Major drugs bust leads to 48 arrests in Spain, Argentina and Italy' (footnote 31, above).

35 'Condenas de 7 a 15 años de prisión por el tráfico de 1.160 kilos de cocaina', Fiscales.gob.ar (23 December 2019), at https://www.fiscales.gob.ar/narcocriminalidad/condenas-de-7-a-15-anos-de-prision-por-el-trafico-de-1-160-kilos-de-cocaina/.

36 'Promotion of Joint Investigation Teams in Latin America', EL PAcCTO (4 December 2020), at https://www.elpaccto.eu/en/news/promotion-of-joint-investigation-teams-in-latin-america/.

37 GAFILAT, 'Mutual Evaluation Report of Peru' (February 2019), Financial Action Task Force, para. 368, at http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-peru-2019.html.

38 Id.

39 Luis Dantón Martínez Corres, 'How a Financial Intelligence Unit is trailblazing anti-corruption enforcement', *The FCPA **Blog*** (24 October 2019), at https://fcpablog.com/2019/10/24/how-a-financial-intelligence-unit-is-trailblazing-anti-corruption-enforcement/.

© Law Business Research 2021

of Mexico's largest steelmaker, Altos Hornos de Mexico.[40] Further, Brazil's Counsel for Financial Activities Control referred 5,273 financial intelligence reports to law enforcement and commenced 12 money laundering and administrative actions between January and September 2019.[41]

However, insufficient resources severely undermine regional FIU anti-corruption efforts. Mexico's FIU operates on a budget of approximately US$7 million to combat the US$50 billion of money laundering in the country each year, and Guatemala's FIU is chronically understaffed.[42] The United States has provided financial support for training and upgraded technical infrastructure, including updated data systems, to FIUs throughout Latin America.[43]

Law enforcement networks

Law enforcement networks regularly bring together officials to exchange ideas and experiences, and to provide real-time collaboration on cross-border investigations. One example is the Latin America and Caribbean Anti-Corruption Law Enforcement Network (LAC LEN), created in 2018 by anti-corruption authorities with the assistance of the OECD's WGB. LAC LEN allows for informal, peer-to-peer exchanges of information and the facilitation of legal assistance.[44] Its inaugural meeting brought together law enforcement officials and attorneys from 14 countries with representatives from the OECD, the Organization of American States, the Inter-American Development Bank and the Iberoamerican Network of Prosecutors against Corruption of the Iberoamerican Association of Public Ministries. A similar network for judges and legal authorities, the Ibero-American Network for International Legal Cooperation (IberRed), was created to optimise legal co-operation in criminal and civil matters between members of the Organization of Ibero-American States[45] and to establish and maintain an updated

40 Anthony Esposito, 'Mexico takes aim at former Pemex CEO in fight against graft', *Reuters* (27 May 2019), at https://www.reuters.com/article/us-ahmsa-mexico/mexico-takes-aim-at-former-pemex-ceo-in-fight-against-graft-idUSKCN1SX1W4.

41 US Department of State, Bureau of International Narcotics and Law Enforcement Affairs, 'International Narcotics Control Strategy Report, Volume II: Money Laundering' (March 2020), at https://www.state.gov/wp-content/uploads/2020/03/Tab-2-INCSR-Vol-2-508.pdf.

42 Andrés Martínez-Fernández, Julia Yansura, 'Money Laundering Could Stifle Latin America's Response to COVID-19', *World Politics Review* (11 June 2020), at https://www.worldpoliticsreview.com/articles/28833/in-latin-america-corruption-and-money-laundering-are-stifling-responses-to-covid-19.

43 'Anti-Money Laundering – U.S. Efforts to Combat Narcotics-Related Money Laundering in the Western Hemisphere', United States Government Accountability Office (August 2017), at https://www.gao.gov/assets/690/686727.pdf.

44 'First meeting of the Latin America and Caribbean Anti-Corruption Law Enforcement Network', OECD (24 October 2018), at https://www.oecd.org/daf/anti-bribery/first-meeting-of-the-latin-america-caribbean-anti-corruption-law-enforcement-network.htm.

45 The Organization of Ibero-American States is an international government body for co-operation between Latin American countries in the fields of education, science, technology and culture in the context of integral development, democracy and regional integration. Full members and observers are all Latin American countries that make up the community comprising Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Guinea Equatorial nations,

© Law Business Research 2021

information system about their different legal systems.[46] In 2020, IberRed entered into an agreement with the European Union Agency for Criminal Justice Cooperation (Eurojust) to provide access for Member States to the Iber@ Secure Communication System, allowing secure and real-time communications between judges, prosecutors and central authorities throughout Latin America and Europe.[47] In June 2021, the Treaty on the Electronic Transmission of Requests of International Judicial Cooperation between Central Authorities, also known as the Medellín Treaty, entered into force following its ratification by Andorra, Cuba and Spain.[48] The Medellín Treaty, which has already been signed by Argentina, Brazil, Chile, Colombia, Ecuador, Paraguay, Portugal and Uruguay, provides a formal mechanism for allowing party states to use the Iber@ platform to expedite the processing and transmission of requests for international legal cooperation.[49]

Comparing the robustness of enforcement regimes and multi-jurisdictional coordination

The level of co-operation by Latin American countries varies depending on the specific investigative and prosecutorial demands (e.g., wide-ranging scandals involving more than one jurisdiction, such as the *Odebrecht* investigation), as well as the commitment and operational infrastructure of law enforcement authorities. Differences in approaches, available resources and technology, and competing timelines can frustrate efforts to build strong and seamless collaboration between agencies. Countries in the region with strong cross-border corruption enforcement, such as Brazil, are characterised by expansive anti-corruption legislation, robust enforcement agencies with skilled investigators and prosecutors, and solid democratic institutions. Others, such as Colombia and Peru, are at the early stages but struggle to marshal the resources, technical capacity or political will to fully develop sustainable programmes for international anti-corruption enforcement co-operation. However, many Latin American countries practise very little international enforcement co-operation. Even when countries have agreed to MLA treaties

Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Portugal, Spain, Uruguay and Venezuela. The headquarters of the General Secretariat is in Madrid, Spain, and there are regional offices in Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru and Uruguay. 'Organization of Ibero-American States (OEI)', Devex, at https://oei.int/quienes-somos/oei (last accessed 30 August 2021).

46 'IberRed (Red iberoamericana de cooperación jurídica internacional)', Conferencie de Ministros de Justicia De Los Paises IberoAmericanos, at https://comjib.org/iberred/ (last accessed 12 August 2020).

47 'Implementing Arrangement to the Memorandum of Understanding between Eurojust and IberRed on the use of the Iber@ Secure Communication System', Eurojust (28 May 2020), at http://eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Implementing%20Arrangement%20to%20the%20MoU%20between%20Eurojust%20and%20IberRed%20%282020%29/2020-05-28_Implementing-arrangement-EJ-IberRed.pdf.

48 'Spain ratifies the Treaty of Medellín allowing its entry into force', Red Iberoamericana de Cooperación Jurídica Internacional (2 June 2021), at https://iberred.notariado.org/en/-/spain-ratifies-the-treaty-of-medellin-allowing-its-entry-into-force.

49 Id.; 'Cuba ratifies the Medellín Treaty.', Red Iberoamericana de Cooperación Jurídica Internacional (27 April 2021), at https://iberred.notariado.org/en/-/cuba-ratifies-the-medellin-treaty.

© Law Business Research 2021

or enacted specific legislation requiring international co-operation (such as Argentina, Chile and Mexico), they often lack adequate resources or procedural mechanisms to fulfil their commitments efficiently and effectively. Argentina serves as a prime example, where because hundreds of cases are handled by the same investigative judge, cases sometimes expire because they have reached the end of the statute of limitations period.[50]

Anti-corruption enforcement efforts temporarily slowed down in Latin America during the covid-19 pandemic, even though the global health crisis increased corruption concerns, particularly with regard to emergency procurement and public spending.[51] The 2021 Capacity to Combat Corruption (CCC) Index indicates that Brazil, Mexico and Colombia experienced reductions in their corruption scores, mainly because of budget cuts and reduced agency independence. Other countries, such as the Dominican Republic, Panama and Ecuador, showed improvements.[52] Numerous corruption scandals have arisen in the region concerning procurement of ventilators and personal protective equipment, which have led to arrests of and resignations by top officials. For example, the Bolivian health minister was arrested for allegedly purchasing ventilators at inflated prices, and similarly, a top adviser to the Panamanian vice president resigned after prosecutors probed the government's planned purchase of overpriced ventilators.[53] Prosecutors in Argentina, Brazil and Colombia have similarly investigated government officials for pandemic-related corruption, including the embezzling of public healthcare funds for covid-19 field hospitals and the purchasing of overpriced surgical masks from politically connected vendors.[54]

Co-operation with US enforcement agencies has also continued throughout the covid-19 crisis, leading to noteworthy FCPA-related resolutions. Collaboration with US enforcement agencies is also likely to increase under the Biden administration. For example, President Biden recently announced efforts to co-operate with Central American officials to address corruption in the Northern Triangle region of Central America (Guatemala, El Salvador and Honduras).[55] All told, it is reasonable to expect anti-corruption efforts will continue to expand in the coming years.

---

50 'Argentina: Follow-up To The Phase 3bis Report & Recommendations' (footnote 31, above).

51 Geert Aalbers, 'Headwinds in the fight against corruption in Latin America', Control Risks (2021), at https://www.controlrisks.com/our-thinking/insights/headwinds-in-the-fight-against-corruption-in-latin-america.

52 Geert Aalbers, 'How has the pandemic affected the anti-corruption fight in Latin America?,' The FCPA Blog (23 August 2021), at https://fcpablog.com/2021/08/23/how-has-the-pandemic-affected-the-anti-corruption-fight-in-latin-america/; 'The Capacity to Combat Corruption (CCC) Index: Assessing Latin America's ability to detect, punish and prevent corruption' (2021), at 2–3, at https://americasquarterly.org/wp-content/uploads/2021/06/CCC_Report_2021.pdf.

53 John F Walsh, Tico Almeida and Margarita Botero, 'Latin America Anti-Bribery Year-in Review: 2020 Developments and Predictions for 2021', WilmerHale (25 March 2021), at 1, at https://www.wilmerhale.com/en/insights/client-alerts/20210319-latin-america-and-foreign-corrupt-practices-act.

54 Id. at 1–2.

55 Id. at 4; Mark Schindler, 'Six Months On: Changes in U.S. Policy toward the Northern Triangle', Center for Strategic and International Studies (20 July 2021), at https://www.csis.org/analysis/six-months-changes-us-policy-toward-northern-triangle.

© Law Business Research 2021

Brazil

Brazilian authorities may provide MLA on the basis of a bilateral treaty, a multilateral treaty or reciprocity, with the majority of incoming and outgoing MLA requests made on the basis of bilateral treaties. The Department of Asset Recovery and International Cooperation, a branch of the Ministry of Justice and Public Security,[56] is responsible for executing MLATs and coordinating Brazilian efforts in co-operating in international criminal investigations.[57] In practice, however, the Federal Police, Federal Prosecution Service (MPF) and the Office of the Comptroller-General are the entities that regularly engage in international co-operation efforts and therefore carry out the largest number of the requests.[58] Brazil is unique in that it publishes monthly statistical reports on requests for international legal co-operation, categorising the number of requests by type, current status and number of countries involved.

Brazil is the region's leader in international co-operation efforts. Between the OECD Anti-Bribery Convention's entry into force in Brazil in 2000 and 2014, Brazilian authorities opened investigations into only three of 14 foreign bribery allegations and prosecuted only one foreign bribery case.[59] However, domestic law enforcement entities have since made significant progress in responding to MLA and information requests from foreign FIUs and other foreign counterparts. The high-profile *Operation Car Wash* investigation has undoubtedly afforded Brazil extensive opportunities for co-operation with foreign authorities. As at 21 January 2021, the MPF reported that it had received 653 MLA requests from more than 40 countries and had sent 597 MLA requests to 58 countries in the context of *Operation Car Wash*.[60] As a result, Brazilian authorities have successfully frozen or seized approximately US$450 million located in overseas bank accounts. These numbers demonstrate the immense progress that Brazilian authorities have made in the past five years and showcase the sophistication of Brazilian intelligence in identifying leads and evidence located overseas. This has been possible because of tools developed by Brazilian law enforcement to tackle bribery schemes with complex multi-jurisdictional components. In recent years, federal police and prosecutorial services have frequently resorted to instruments such as the Register for Clients of the National Financial System and the Banking Transactions Investigation System to identify illicit financial flows, beneficial ownership and other important evidence.[61]

56 'Brazil: Follow-Up To The Phase 3 Report & Recommendations', OECD Working Group on Bribery (February 2017), at https://www.oecd.org/corruption/anti-bribery/Brazil-Phase-3-Written-Follow-Up-Report-ENG.pdf.

57 'Country Review Report of Brazil', UNODC (19 January 2017), at 57, at https://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2017_01_19_Brazil_Final_Country_Report.pdf.

58 'Phase 3 Report on Implementing the OECD Anti-Bribery Convention in Brazil', OECD Working Group on Bribery (October 2014), at https://www.oecd.org/daf/anti-bribery/Brazil-Phase-3-Report-EN.pdf, at 25–26.

59 Id.

60 'Efeitos no Exterior (Cooperação ativa e passiva na Lava Jato)', Ministério Público Federal (MPF), at www.mpf.mp.br/grandes-casos/lava-jato/efeitos-no-exterior.

61 Vladimir Aras, 'International Cooperation and Other Catalysts for Anti-Corruption Prosecution', *JOTA* (29 May 2019), at https://www.jota.info/especiais/international-cooperation-and-other-catalysts-for-anticorruption-prosecution-29052019.

© Law Business Research 2021

Notably, however, the covid-19 pandemic and related budgetary challenges may have created setbacks in Brazil's anti-corruption efforts, particularly as a result of relaxed public contracting requirements implemented to maintain profitability of businesses during the crisis.[62] In addition, recent appointments by President Bolsonaro to the Federal Police and Federal Public Ministry have led to a decrease in the perceived independence of Brazil's anti-corruption agencies and chief prosecutor's office. It is unclear whether these appointments will affect anti-corruption efforts in Brazil or more broadly in the region.[63]

Nonetheless, Brazil's cooperation with US authorities has continued throughout the pandemic and has resulted in high-profile resolutions relating to bribery schemes in Brazil and other countries in Latin America. These include the US$16.6 million settlement with asphalt company Sargeant Marine Inc for bribes made to foreign officials in Brazil, Venezuela and Ecuador; Vitol Inc's US$165 million settlement with both US and Brazilian authorities for its oil contracts bribery scheme in Brazil; and the US$256 million settlement of Brazilian conglomerate J&F for its scheme to bribe foreign officials in Brazil.[64] Anti-corruption co-operation efforts between Brazil and the United States are likely to continue apace throughout the Biden administration.

Colombia

Colombia's legal framework for MLA is laid out in Articles 484 to 489 of the Colombian Code of Criminal Procedure, and a number of multilateral and bilateral MLATs with several countries, including Argentina, Brazil, France, Mexico, Spain and the United Kingdom. If Colombia does not have an MLAT with a foreign country, international legal instruments such as the UNCAC and the IACAC may provide a legal basis for Colombian authorities to request and obtain crucial evidence and assistance to advance corruption investigations. Notably, Colombia data collected via MLA does not appear updated or comprehensive, according to the most recent OECD WGB report.[65]

The Superintendency of Corporations is Colombia's independent agency for conducting administrative investigations of legal persons in respect of acts of bribery. Colombia has taken concrete steps to enhance the Superintendency's capacity to effectively engage in international co-operation. It has concluded an agreement with Brazil's administrative authority in charge of enforcement against legal persons. From 2017 to 2019, the Superintendency signed two MLATs for direct information exchange in transnational bribery investigations with criminal law enforcement authorities in Peru (Public Ministry) and the United Kingdom (Serious Fraud Office), and reported 'aggressively'

62 Antonio Carlos Vasconcellos Nóbrega and Vanessa Boechat, 'The Effects of Covid-19 on Compliance Programmes in Brazil', Global Investigations Review (13 October 2020), at https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2021/article/the-effects-of-covid-19-compliance-programmes-in-brazil.

63 'The Capacity to Combat Corruption (CCC) Index: Assessing Latin America's ability to detect, punish and prevent corruption' (2021), at 18, at https://americasquarterly.org/wp-content/uploads/2021/06/CCC_Report_2021.pdf.

64 Id., at 3–4.

65 'Implementing the OECD Anti-Bribery Convention – Phase 3 Report: Colombia', at 52 (12 December 2019), at www.oecd.org/corruption/Colombia-Phase-3-Report-ENG.pdf.

© Law Business Research 2021

pursuing the establishment of similar agreements with as many countries as possible, prioritising those in Latin America.[66]

Colombian authorities are increasingly able to resort to targeted legislation, such as the revised Asset Forfeiture Law and the Transnational Corruption Act (2016), to meet specific investigative needs. These have and will continue to enhance authorities' ability to keep up with criminality. In a recent corruption case, Colombian authorities successfully used the Asset Forfeiture Law to work with a foreign authority to seize proceeds generated in Colombia and moved to the foreign country. Additionally, Colombia has pursued numerous investigations under its Transnational Corruption Act, which creates administrative liability for corporations involved in foreign bribery.

International monitoring bodies acknowledge Colombia's initial progress. In its most recent Colombia report, the OECD WGB stated that the country appeared to provide timely assistance to foreign partners. The WGB pointed to a case in which Colombian authorities executed a foreign authority's MLA request for bank and company records within five months of receiving the request, which was no more than the time needed to obtain similar information in a domestic procedure.[67]

Like many of its neighbours, Colombia's corruption risk profile has increased during the pandemic and appears to represent a setback in anti-corruption efforts. The 2021 CCC Index indicates that Colombia's scores for independence of the chief public prosecutor and anti-corruption agencies have dropped, mainly because of President Iván Duque's recent placement of less independent officials in positions such as ombudsman, attorney general and inspector general. Emergency spending relating to the pandemic has also led to irregularities in public contracting and reports of possible corruption.[68]

Peru

Article 508(1) of the Code of Criminal Procedure (CPC) allows Peru to seek and provide MLA in criminal matters through a treaty or the principle of reciprocity, and as at 2021, Peru had engaged 20 countries in bilateral MLATs, including several Latin American countries that are part of the OECD Anti-Bribery Convention (Argentina, Colombia, Brazil and Mexico).[69] If a treaty does not apply, Articles 508 to 512 and 528 to 537 of the CPC provide the legal framework.[70] Peru's Public Prosecutor's Office is the central authority for MLA requests and receives additional support from the Ministry for Foreign Affairs pursuant to Article 512 of the CPC.[71] Peru requires dual criminality for MLA requests seeking asset tracing, freezing and seizing bank accounts and criminal assets, intercepting communications, and other measures that limit individual rights, pursuant to

66 Id., at 52–53.

67 Id.

68 'The Capacity to Combat Corruption (CCC) Index: Assessing Latin America's ability to detect, punish and prevent corruption' (2021), at 20, at https://americasquarterly.org/wp-content/uploads/2021/06/CCC_Report_2021.pdf.

69 Phase 2 Report: Peru, OECD Anti-Bribery Convention (30 June 2021), at 44, at https://www.oecd.org/daf/anti-bribery/peru-phase-2-report.pdf.

70 Id.

71 Id.

© Law Business Research 2021

Articles 511(1)(h) and 529(2) of the CPC.[72] Peru is also party to the OECD Anti-Bribery Convention, the UNCAC, the IACAC and the Inter-American Convention on Mutual Assistance in Criminal Matters.[73]

In the past two decades, Peru has introduced various initiatives with the goal of remedying the pattern and practice of corruption that accompanied the Fujimori presidency. In 2010, the Presidency of the Council of Ministers established the High-Level Anti-Corruption Commission (CAN), which created a national anti-corruption plan operating from 2012 until 2016 with the objective of preventing and combating corruption via coordinated action. One lasting benefit of the CAN is the creation of a digital platform that enables coordination between Peruvian anti-corruption bodies via information-sharing technology.[74] In 2016, Peru became a full member of the OECD WGB.[75] Peru has also committed to co-operating in joint investigations relating to the *Odebrecht* scandal, having signed the Brasilia Declaration on International Joint Investigations in 2017.[76] To date, Peru has made 274 requests to Brazil and has received three from Brazil in relation to the scandal.[77] Peru has made progress in *Operation Car Wash* enforcement efforts. Its *Lava Jato* Special Team, a dedicated team of prosecutors responsible for investigating bribes relating to *Operation Car Wash*, has increased the scale of prosecution of Peruvian politicians and officials at the highest level starting in 2017.[78] Several high-ranking Peruvian officials, including three former presidents, have been arrested and are currently under investigation. Among them are former president Ollanta Humala and his wife, Nadine Heredia, who Peruvian prosecutors accuse of awarding state contracts to Odebrecht in exchange for campaign contributions.[79] Peru also issued an extradition request to the United States for former president Alejandro Toledo and his wife, Eliane Karp, in July 2019 for money laundering in connection with bribes allegedly received from Odebrecht.[80] As at September 2021, Toledo continued to challenge his

72 Id., at 37.

73 Id., at 38.

74 Cristina Figaredo, 'Tackling corruption in Peru (2010-2018)', Centre for Public Impact (30 October 2018), at https://www.centreforpublicimpact.org/case-study/tackling-corruption-peru/.

75 'La lucha contra el soborno transanacional en America Latina y el Caribe', OECD (2018), at https://www.oecd.org/corruption/anti-bribery/OECD-Brochure-Latin-America-Caribbean-Anti-Corruption-Initiative-ESP.pdf.

76 Id.; 'Latin American prosecutors join forces on Odebrecht bribes', *Reuters* (17 February 2017), at https://www.reuters.com/article/us-brazil-corruption-latinamerica/latin-american-prosecutors-join-forces-on-odebrecht-bribes-idUSKBN15W2H7.

77 'Efeitos no Exterior (Cooperação ativa e passiva na Lava Jato)', MPF (footnote 60, above).

78 Phase 2 Report: Peru, OECD Anti-Bribery Convention (30 June 2021), at 33–34, at https://www.oecd.org/daf/anti-bribery/peru-phase-2-report.pdf.

79 'Prosecutor requests 20 years in jail for ex-Peru president', *AP News* (7 May 2019), at https://apnews.com/article/ollanta-humala-caribbean-latin-america-nadine-heredia-peru-288d6b884ff841d082d8968cbb61712e; 'Peru's former first lady faces jail over Odebrecht corruption', International Consortium of Investigative Journalists (12 March 2020), at https://www.icij.org/investigations/bribery-division/perus-former-first-lady-faces-jail-over-odebrecht-corruption/.

80 Nicholas Iovino, 'Judge Advances Extradition Case Against Ex-Peru President', (4 September 2020), at https://www.courthousenews.com/judge-advances-extradition-case-against-ex-peru-president/.

© Law Business Research 2021

extradition in California, where he was released on bail in March 2020 owing to health concerns stemming from the covid-19 pandemic.[81] At the same time, former president Pedro Pablo Kuczynski remained under house arrest while awaiting trial on allegations that he improperly influenced the awarding of highway construction contracts in exchange for payments from Odebrecht while serving as a cabinet minister in the Toledo administration.[82] A fourth former president, Alan Garcia, killed himself in April 2019 when police arrived at his home to arrest him based on similar allegations.[83]

Additionally, on 1 January 2018, the Peruvian Congress enacted Law 30424, which introduces corporate liability for existing criminal offences relating to corruption, money laundering and financing of terrorism.[84] The Law is applicable to legal entities that bribe public servants or officials either domestically or internationally.[85]

Even as Peru continues to make progress in its efforts to combat foreign bribery, there is still room for improvement, according to a June 2021 report by the OECD WGB. In that report, the WGB identified the following points of improvement to fortify Peru's foreign anti-bribery enforcement: (1) protection of prosecutors from unjustified removal from cases; (2) reduction of provisional and excess numbers of judges and prosecutors; (3) protection of whistleblowers and promotion of whistleblower culture; and (4) better coordination and oversight of MLA requests to other countries.[86] To address the WGB's recommendations, Peruvian officials have indicated that the country will commit to improving its statistical collection of MLA and money-laundering enforcement.[87]

Argentina

Argentina collaborates with foreign authorities in investigations through bilateral, regional and multilateral treaties. As of 2017, bilateral MLATs are in force with 16 countries, with

81 'Defensa de Alejandro Toledo usa su "falta de paciencia" como prueba en juicio', *Yahoo!Noticias* (10 September 2020), at https://es-us.noticias.yahoo.com/defensa-alejandro-toledo-usa-falta-221813258.html.

82 María Isabel Álvarez, 'PPK: Fiscalía pide impedimento de salida del país para expresidente por caso Interoceánica', *El Comercio* (9 September 2021), at https://elcomercio.pe/politica/justicia/ppk-fiscalia-pide-orden-de-impedimento-de-salida-del-pais-contra-pedro-pablo-kuczynski-por-caso-interoceanica-jose-domingo-perez-equipo-especial-noticia/?ref=ecr.

83 'Peru's former first lady faces jail over Odebrecht corruption', International Consortium of Investigative Journalists (footnote 79, above).

84 Matteson Ellis, 'Peru Introduces Corporate Liability for Corruption Offenses with a Compliance Program Defense', *FCPAméricas Blog* (2 April 2018), at https://fcpamericas.com/english/anti-corruption-compliance/peru-introduces-corporate-liability-corruption-offenses-compliance-program-defense/# m.

85 Id.

86 OECD, 'Peru has strengthened domestic corruption enforcement, now must maintain momentum and increase foreign bribery awareness and enforcement' (30 June 2021), at https://www.oecd.org/countries/peru/peru-has-strengthened-domestic-corruption-enforcement-must-maintain-momentum-and-increase-foreign-bribery-awareness-and-enforcement.htm; 'Implementing the OECD Anti-Bribery Convention – Phase 2 Report: Peru', OECD (30 June 2021), at https://www.oecd.org/daf/anti-bribery/peru-phase-2-report.pdf.

87 Id., at 5.

© Law Business Research 2021

more being negotiated.[88] Argentina has received requests for MLA under the OECD Anti-Bribery Convention, the UNCAC and the IACAC. Other applicable multilateral treaties include Law No. 26004 on the Mutual Assistance Agreement in Criminal Matters of Mercosur (Argentina, Brazil, Paraguay, Uruguay, Bolivia and Chile) and Law No. 26139 on the Inter-American Convention on Mutual Legal Assistance in Criminal Matters.[89] As at 2021, Argentina has also signed 20 double taxation agreements and 28 tax information exchange agreements to assist in the investigation and prosecution of international tax crimes.[90] For countries that do not have a treaty, Argentina 'shall afford the widest possible measure of assistance' under Law No. 24767 on International Co-operation in Criminal Matters on condition of reciprocity.[91] This Law also regulates extradition and other forms of assistance in criminal investigations.

Under Argentine law, the country can grant coercive measures pursuant to an MLA request (e.g., search and seizure, wiretapping and surveillance) if the underlying conduct is a crime in both participating states.[92] This is subject to restrictions regarding measures that may violate individual privacy rights guaranteed by Argentina. Argentina's MLA is limited to criminal actions; it cannot provide MLA for use in civil or administrative liability against legal persons for foreign bribery.[93] In March 2018, Argentina passed Law No. 27401, establishing criminal liability for corporations that have bribed domestic or foreign officials, with protection against liability when self-reporting.[94]

Numerous challenges arise in requesting MLA from Argentina. First, requests are often significantly delayed: the average time for completing incoming requests is 4.6 months. As at July 2019, Argentina had 83 outstanding outgoing MLA requests in corruption cases, some of which came from five foreign bribery investigations that opened in 2016.[95] Further, investigative judges responsible for leading foreign bribery investigations are under-resourced; there are few judges available to handle these types of cases. In Buenos Aires, 12 investigative judges handle all cases under federal jurisdiction – one judge disclosed during an OECD investigation that he has 400 to 500 ongoing cases in addition to a complex economic foreign bribery case.[96] Argentina neverthe-

88 'Argentina: Follow-up To The Phase 3bis Report & Recommendations' (footnote 31, above).

89 'Argentina', *The International Investigations Review* (The Law Reviews, 10th Edition, August 2019), at https://thelawreviews.co.uk/edition/the-international-investigations-review-edition-10/1229374/argentina.

90 'Fighting Tax Crime – The Ten Global Principles', Country Chapters (Second Edition), OECD (4 June 2021), at https://www.oecd.org/tax/crime/fighting-tax-crime-the-ten-global-principles-second-edition-country-chapters.pdf?_ga=2.68991122.241443825.1630200732-1328061632.1630200732.

91 'Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-Step Guide', 2012, G20 (2012) (footnote 19, above).

92 'Argentina: Follow-up To The Phase 3bis Report & Recommendations' (footnote 31, above).

93 Id.

94 Matteson Ellis, 'Argentina Introduces Corporate Liability and Compliance Standards in New Anti-Corruption Law', *FCPAméricas Blog* (6 March 2018), at https://fcpamericas.com/English/anti-corruption-compliance/argentina-introduces-corporate-liability-compliance-standards-anti-corruption-law/#.

95 'Argentina: Follow-up To The Phase 3bis Report & Recommendations' (footnote 31, above).

96 Id.

© Law Business Research 2021

less has resources available to pursue MLA concerns. It is a member of both IberRed and the Hemispheric Network for Legal Cooperation on Criminal Matters (under the Organization of American States).[97]

In 2021, Argentina has experienced reductions in the independence of its chief public prosecutor's office and anti-corruption agencies. International watchdogs have also raised concerns about former president and current vice president Cristina Fernández de Kirchner's adverse influence in enforcement efforts, noting that she is a defendant in multiple corruption investigations.[98]

Chile

Although Chile has not enacted any law governing international co-operation, a few procedural rules regulate MLATs and are applied in the execution of MLA.[99] Chile mainly requests international co-operation with Latin American countries, relying most frequently on Argentina, Peru, Colombia and Bolivia.[100] Chile's anti-corruption statute, Law No. 19913, creates the Financial Analysis Unit and modifies various provisions concerning money laundering in view of their importance in international affairs. Under Article Two, the Unit's function is to share information with international counterparts.[101] Chile also has national legislation condemning the bribery of domestic and foreign public officials.[102] Moreover, Chile is a member of the Mutual Administrative Assistance in Tax Matters and has exchange of information relationships with more than 36 other jurisdictions through bilateral tax treaties and tax information exchange agreements. However, to date, the Chilean Tax Crime Department of Sensitive and International Investigations has had no MLA requirements within its jurisdiction.[103]

According to a recent OECD report, Chile's anti-corruption measures have improved in recent years.[104] Starting in 2016, Chilean tax authorities have collaborated with the US Securities and Exchange Commission to investigate illicit payments made by the Chilean Chemical and Mining Society, which led to various settlements with the

97 Id.

98 'The Capacity to Combat Corruption (CCC) Index: Assessing Latin America's ability to detect, punish and prevent corruption' (2021), at 16 (2021), at https://americasquarterly.org/wp-content/uploads/2021/06/CCC_Report_2021.pdf.

99 'Public Prosecutor's Office of Chile', FISCALIA, at https://www.unodc.org/documents/international-cooperation/News_and_events/CHILE_UNTOC_Contributions.pdf.

100 Id.

101 'Hemispheric Network for Legal Cooperation on Criminal Matters', OAS, at http://web.oas.org/mla/en/Pages/countries_bilateral.aspx?ISO=CHL; https://web.oas.org/mla/en/G_Countries_MLA/chl_mla_leg_es.pdf (last accessed 14 August 2020).

102 Chilean Criminal Code, Articles 248 to 251.

103 'Fighting Tax Crime – The Ten Global Principles', Country Chapters (Second Edition), OECD (4 June 2021) (footnote 90, above), at 90–91.

104 See 'Implementing the OECD Anti-Bribery Convention; Phase 4 Report: Chile', OECD, at 67 (13 December 2018), at https://www.oecd.org/corruption/anti-bribery/OECD-Chile-Phase-4-Report-ENG.pdf.

© Law Business Research 2021

US government.[105] Additionally, in November 2016, the Chilean Court of Appeal convicted Victor Lizarraga for bribing a Korean adviser of a military attaché for introductions to Korean companies seeking contracts from the Chilean military.[106] The conviction marked Chile's first foreign bribery conviction against a natural person.[107] Despite having concluded two successful bribery enforcement actions and reopening cases the OECD deemed insufficiently tried, the OECD still recommended that Chile '(a) ensure that it assess credible allegations of foreign bribery when they surface, and seriously investigate this offence in Chile and abroad; and (b) use proactive steps to gather information from diverse sources to increase sources of allegations and enhance investigations'.[108] Although Chile has enjoyed positive experiences in obtaining evidence from foreign companies for domestic suits or in requesting MLA from other states, the process of obtaining MLA in Chile has proven to be cumbersome, resulting in unnecessary delay and rendering Chile's success with MLA one-sided.[109]

Mexico

Mexico is a party to the UNCAC and the IACAC, and boasts the largest number of international treaty agreements involving MLA: at least 30 MLATs and 38 extradition treaties.[110] It provides MLA without an applicable treaty where there is reciprocity and dual criminality under its International Extradition Law (Articles 3, 5, 6, 15 and 16).[111] Under the United States–Mexico–Canada Agreement's (USMCA) anti-corruption chapter on enforcement co-operation, signatories recognise the importance of co-operation, coordination and exchange of information among their respective anti-corruption law enforcement agencies to foster effective measures to prevent, detect and deter bribery and corruption. The USMCA also imposes enhanced anti-corruption requirements on signatory parties. These focus on strengthening international co-operation between law enforcement agencies and require each signatory country to criminalise embezzlement

105 Waithera Junghae, 'SQM Internal Probe Finds Potential Improper Payments', *Global Investigations Review* (25 April 2016), at https://globalinvestigationsreview.com/article/1035471/sqm-internal-probe-finds-potential-improper-payments; US Securities and Exchange Commission, press release, 'Chemical and Mining Company in Chile Paying $30 Million to Resolve FCPA Cases' (13 January 2017), at https://www.sec.gov/news/pressrelease/2017-13.html; US Department of Justice, press release, 'Chilean Chemicals and Mining Company Agrees to Pay More Than $15 Million to Resolve Foreign Corrupt Practices Act Charges' (13 January 2017), at https://www.justice.gov/opa/pr/chilean-chemicals-and-mining-company-agrees-pay-more-15-million-resolve-foreign-corrupt.

106 'Implementing the OECD Anti-Bribery Convention; Phase 4 Report: Chile' (footnote 104, above), at 30.

107 Id.

108 Id., at 68.

109 Id., at 31.

110 Extradición, Supreme Corte de Justicia de la Nación, at https://www.scjn.gob.mx/tratados-internacionales/caracter-especial/extradicion (last visited 29 August 2021); 'Phase 3 Report on Implementing the OECD Anti-Bribery Convention in Mexico', OECD (October 2011), at 31, at https://www.oecd.org/daf/anti-bribery/Mexicophase3reportEN.pdf.

111 Id., at 31.

© Law Business Research 2021

and misappropriation of funds by public officials to the extent that this type of conduct affects international trade or investment.

Despite having many bilateral MLATs, meaningful precedents of cases in which Mexican enforcers have co-operated with peers in other jurisdictions to crack down on cross-border corruption cases are limited. MLA requests are governed by the National Code of Criminal Procedure, and the Directorate of International Legal Assistance is responsible for receiving, forwarding and overseeing MLA requests.[112] MLA requests experience significant delays in Mexico because of bureaucratic procedures, with an average waiting time of approximately eight to nine months.[113] The development of institutional capabilities is perhaps Mexico's greatest challenge for anti-corruption enforcement.[114] Domestic implementation of the National Anti-corruption System has been slow, leaving foreign jurisdictions with an underdeveloped partner in Mexico.[115]

In the *Odebrecht* investigations, Mexico has not been able to bring to justice any key public officers or private parties. Additionally, several cases involve consent decrees and similar agreements between corporations and individuals and US authorities for corruption involving Mexican government agencies, without Mexican enforcement.[116] Major investigations in the past, including the US DOJ's seven-year investigation of Walmart, have been led by the US DOJ with almost no participation by Mexico counterparts.

However, Mexico has taken action that suggests improvements in international co-operation. It has hosted summits concerning international co-operation in detecting and investigating foreign bribery. Further, Mexican authorities developed an electronic case management system called Justici@.Net, which provides a case management system to systematise legal assistance procedures for criminal proceedings including MLA procedures and processes[117] In June 2016, Mexico amended Articles 421 and 422 of its National Code of Criminal Procedure to 'provide for the autonomous liability of legal and natural persons for foreign bribery, and to allow legal persons to be held liable for criminal offences when they fail to comply with due controls in their organizations'.[118] The

112 Id., at 37.

113 Id.

114 Luis Dantón Martínez Corres, Thomas S Heather, Marta Loubet and Juan José Paullada Eguirao, 'Mexico: At a turning point in Anti-corruption Investigations and Enforcement', *Global Investigations Review* (19 August 2019), at https://globalinvestigationsreview.com/benchmarking/americas-investigations-review-2020/1196469/mexico-at-a-turning-point-in-anti-corruption-investigations-and-enforcement.

115 Jaclyn Jaeger, 'Mexico's war on corruption an uphill battle for compliance officers', *Compliance Week* (29 June 2020), at https://www.complianceweek.com/anti-corruption/mexicos-war-on-corruption-an-uphill-battle-for-compliance-officers/29127.article.

116 'Bribery & Corruption 2020: Mexico', Global Legal Insights, at https://www.globallegalinsights.com/practice-areas/bribery-and-corruption-laws-and-regulations/mexico.

117 'Comunicado FGR DPE/1098/19. FGR en Jalisco reafirma conocimientos en el sistema Informático de Justici@net', Fiscalía General de la Republica (29 April 2019), at https://www.gob.mx/fgr/prensa/comunicado-fgr-dpe-1098-19-fgr-en-jalisco-reafirma-conocimientos-en-el-sistema-informatico-de-justici-net; 'Implementing the OECD Anti-Bribery Convention – Phase 4 Report: Mexico', OECD, at 37 (19 October 2018), at http://www.oecd.org/corruption/anti-bribery/OECD-Mexico-Phase-4-Report-ENG.pdf.

118 'Implementing the OECD Anti-Bribery Convention – Phase 4 Report: Mexico', OECD (footnote 117, above), at 40.

© Law Business Research 2021

General Law on Administrative Responsibility, enacted in July 2017, introduces corporate administrative liability of public officials and private natural and legal persons for 'serious' and 'non-serious' administrative offences, with Articles 4, 24 and 25 specifically creating corporate liability for these offences.

During the covid-19 crisis, anti-corruption efforts appear to have receded in light of austerity cuts in public sector salaries.[119] These measures have also led to a decline in the independence, transparency and efficiency of anti-corruption agencies, partly because several public procurement entities and trust funds have been dismantled and centralised under the executive branch during the pandemic.[120] Nonetheless, there are indications of continued efforts to expand anti-corruption enforcement and collaboration, particularly in light of the Biden administration's efforts to fight smuggling and trafficking into the United States at the border with Mexico. In June 2021, Vice President Kamala Harris had a meeting with the Guatemalan and Mexican presidents to attempt to secure greater co-operation on border security.[121] While these talks remain in progress, they signal efforts to continue promoting international co-operation to address cross-border corruption and crime.

Conclusion

International co-operation has become a valuable enforcement tool in Latin America with various formal and informal mechanisms available to facilitate it. During the past two decades, Latin American countries have increased participation in multilateral initiatives designed to combat corruption and engaged the use of MLA, MOUs and JITs across several jurisdictions. These engagements often result in the adoption of established and successful international methods in investigating bribery and other forms of corruption.

The jurisdictions discussed have seen changes at the domestic level reflected in an increase in the cross-jurisdictional exchange of information, the development of electronic tools and databases to facilitate carrying out investigations generally, and substantive changes to bribery and anti-corruption laws. Although countries in the region differ in the extent to which they rely on tools to address corruption, the general trend of reliance is moving upwards. Understanding the coordinative practices of Latin American jurisdictions facilitates the investigative process and helps with managing expectations throughout the life of an investigation.

119 'Status of Latin America's Anti-corruption Fight amid Health and Political Challenges', Congressional Research Services (April 2020), at https://sgp.fas.org/crs/row/IN11350.pdf.

120 'The Capacity to Combat Corruption (CCC) Index: Assessing Latin America's ability to detect, punish and prevent corruption' (2021), at 28, at https://americasquarterly.org/wp-content/uploads/2021/06/CCC_Report_2021.pdf.

121 Alexandra Jaffe and Christopher Sherman, 'Harris targets corruption, immigration on Latin America trip', *AP News* (6 June 2021), at https://apnews.com/article/immigration-health-coronavirus-pandemic-business-government-and-politics-50aa1b6b8df560f6dcb5666ed4f6fd63.

© Law Business Research 2021

4

North America Overview

John D Buretta[1]

In late 2018, Canada, Mexico and the United States entered into the aptly named United States-Mexico-Canada Agreement. This Agreement, which imposes obligations on signatory countries to enforce anti-corruption laws, signalled the beginning of a renewed effort to coordinate prosecution efforts across North American borders. The winter of 2018 also saw a convergence at the doorstep of the United States District Court for the Eastern District of New York of investigative matters spanning the United States, Canada and Mexico. As federal prosecutors were preparing for trial against the Mexican drug cartel leader Joaquín Archivaldo Guzmán Loera, other prosecutors in the District were preparing for an extradition battle relating to Meng Wanzhou, a Chinese national and Huawei executive arrested in Canada on a US federal warrant seeking her extradition to the United States on charges of bank fraud, theft of trade secrets and sanctions evasion. These two matters, among others discussed below, reflect the expanding multilateral nature of enforcement actions in North America, and shed further light on authorities' ability to gather evidence, seek extradition and otherwise coordinate with authorities around the world. A nuanced understanding of the progress and playbook on North American corporate enforcement continues to be critical.

The United States-Mexico-Canada Agreement

In late 2018, each country in North America agreed to abide by the United States-Mexico-Canada Agreement, a tripartite treaty that contains an entire chapter on anti-corruption enforcement and compliance.[2] Subsequently, there was a multi-step domestic ratification

1 John D Buretta is a partner in the litigation department at Cravath, Swaine & Moore LLP. The information in this chapter was accurate as at November 2020.

2 Kara Brockmeyer, Andrew M Levine, Marisa R Taney and Victoria L Recalde, 'NAFTA Replacement Adds Anti-Corruption Provisions', *FCPA Update*, Vol. 10, No. 4 (November 2018).

© Law Business Research 2021

process, in which each country considered any necessary changes to domestic laws and made any required amendments through implementing legislation.[3] The Agreement officially entered into force on 1 July 2020.[4] It imposes a range of obligations on signatory countries, effectively to enforce anti-corruption laws and to enact legislation in support of anti-corruption efforts.[5] The Agreement obliges each country to enforce its anti-corruption laws adequately through active prosecution, and provides clear, uniform definitions for terms, such as illicit enrichment and embezzlement.[6] Importantly, it also requires co-operation between the United States, Mexico and Canada, both in sharing resources and experience and in the exchange of information to prevent, detect and deter bribery and corruption.[7] The Agreement further extends to the promotion of integrity, honesty and responsibility among public officials of the signatory nations.

Co-operation between the United States and Mexico

Recent cross-border interactions

Conviction of Joaquín Archivaldo Guzmán Loera

In perhaps the most high-profile conviction of a Mexican citizen by the United States in recent memory, in February 2019, Joaquín Archivaldo Guzmán Loera (known as El Chapo) was convicted by a federal jury in Brooklyn of being a principal leader of a continuing criminal enterprise – the Mexican organised crime syndicate known as the *Sinaloa* cartel – on charges that included 26 drug-related violations and one of conspiracy to commit murder.[8] The case of El Chapo was investigated by the US Drug Enforcement Agency (DEA), the US Immigration and Customs Enforcement (ICE) and the Federal Bureau of Investigation, working in close consultation with their counterpart authorities in Mexico.[9]

Building the case against El Chapo necessarily required extensive co-operation between authorities in the United States and Mexico. The *Sinaloa* cartel was built on border crossings – cartel members smuggled narcotics from Mexico to wholesale distributors in the United States, then transported billions of illicit dollars back across the border to the Sinaloa area of Mexico – so marshalling evidence required monitoring activity and gathering evidence that spanned a significant geographical range.[10] Throughout the 2000s, officials from both countries worked to build a case against El Chapo, from money

3 Id.

4 US Customs & Border Protection, 'U.S.-Mexico-Canada Agreement (USMCA)' (1 July 2020), at cbp.gov/trade/priority-issues/trade-agreements/free-trade-agreements/USMCA.

5 United States-Mexico-Canada Agreement, Article 27.

6 Id.

7 Id.

8 US Department of Justice (DOJ) press release (12 February 2019), 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges', at https://www.justice.gov/usao-edny/pr/joaquin-el-chapo-guzman-sinaloa-cartel-leader-convicted-running-continuing-criminal.

9 Id.

10 Id.

© Law Business Research 2021

laundering to murder charges, and worked for years to pinpoint his exact location.[11] On 22 February 2014, Mexican marines, with co-operation from US government agencies, arrested El Chapo in Mazatlán, Mexico.[12]

Following the second of El Chapo's two escapes from prison, Mexican officials, sharing intelligence with their US counterparts, together engaged in a manhunt and recaptured him.[13] Despite a history of publicly stating that El Chapo would serve out his sentence in Mexico, the Mexican government subsequently agreed to extradite the cartel leader to the United States to face charges in the Eastern District of New York.[14] The extradition process was not without conflict, however. Mexico outlawed capital punishment in 1975 and has remained steadfast in its refusal to extradite suspects who face the death penalty in the United States.[15] US officials agreed to take the death penalty off the table.[16]

Following his extradition on 19 January 2017, El Chapo was due to stand trial in the United States, which would prove to be another testament to the advanced co-operation between Mexican and US authorities.[17] The evidence presented at El Chapo's trial included testimony from 14 co-operating witnesses, narcotics seizures, weapons, ledgers, text messages, videos, photographs and intercepted phone recordings.[18] The co-operation of witnesses was crucial to building the case against El Chapo. This was particularly true of Vicente Zambada-Niebla, a high-ranking member of the cartel and the son of El Chapo's cartel partner, who was extradited from Mexico to the United States and provided critical testimony about the inner workings of the criminal enterprise.[19]

Following El Chapo's conviction, DEA Acting Administrator Uttam Dhillon stated that the 'success of [the] case is a testament to the strength of [the United States']

11 Noah Hurowitz, 'Inside the Trial of El Chapo', Rolling Stone (4 November 2018), at https://www.rollingstone.com/culture/culture-features/el-chapo-trial-guzman-brooklyn-court-sinaloa-cartel-751035/.

12 Randal C Archibold and Ginger Thompson, 'El Chapo, Most-Wanted Drug Lord, Is Captured in Mexico', *The New York Times* (22 February 2014), at https://www.nytimes.com/2014/02/23/world/americas/joaquin-guzman-loera-sinaloa-drug-cartel-leader-is-captured-in-mexico.html.

13 Azam Ahmed, 'El Chapo Case Draws Mexico Closer to U.S.', *The New York Times* (11 January 2016), at https://www.nytimes.com/2016/01/12/world/americas/el-chapo-case-draws-mexico-closer-to-us.html?module=inline.

14 Azam Ahmed, 'El Chapo. Mexican Drug Kingpin, Is Extradited to U.S.', *The New York Times* (19 January 2017), at https://www.nytimes.com/2017/01/19/world/el-chapo-extradited-mexico.html.

15 Emily Edmonds-Poli, David A Shirk, 'Extradition as a Tool for International Cooperation: Lessons from the U.S.-Mexico Relationship', *Maryland Journal of International Law,* Volume 33, Issue 1, 215, 226 (2018).

16 Id.

17 Azam Ahmed, 'El Chapo. Mexican Drug Kingpin, Is Extradited to U.S.' (footnote 14, above).

18 US DOJ press release, 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges' (footnote 8, above).

19 Jason Meisner, 'Witness Against "El Chapo" Given 15 Years in Prison in Chicago for Key Role in Trafficking Cocaine, Heroin for Cartel', ***Chicago Tribune*** (30 May 2019), at https://www.chicagotribune.com/news/breaking/ct-met-el-chapo-witness-mexican-cartel-sentencing-20190529-story.html.

© Law Business Research 2021

relationship with Mexican counterparts'.[20] The strength of this relationship was tested at each stage of the enforcement action, from building the case until conviction at trial.

Discovery of cross-border drug tunnel

Another example of bilateral co-operation and investigation is the discovery in March 2020 of an underground tunnel more than 2,000 feet in length and running from a warehouse in Tijuana, Mexico, to a warehouse in San Diego, California.[21]

The tunnel was uncovered by federal agents on the San Diego Tunnel Task Force, an investigative team comprised of agents from ICE, DEA, the US Border Patrol and the US Attorney's Office.[22] After developing information about a transnational tunnel used for drug trafficking, the Task Force worked with Mexico's Attorney General's Office and Secretary of Defence to locate the tunnel entrance.[23] To date, no arrests have been made in connection with the discovery, which authorities classify as part of an ongoing investigation, but agents did seize approximately US$26.9 million worth of illegal drugs from the tunnel.[24]

Past cross-border investigations with Mexico

Although El Chapo's trial and conviction may present the most high-profile example, sustained co-operation between US and Mexican authorities has been evident in corporate investigations during the past few years, and may well expand as Mexico enhances its enforcement tools and efforts.

In December 2016, the US Department of Justice (DOJ) secured guilty pleas from six individuals – four business persons employed by Hunt Pan Am, a Houston-based company that provides aircraft maintenance and related services, and two former Mexican government officials – in a cross-border bribery scheme.[25] The criminal proceeding, which was investigated by ICE and the Internal Revenue Service, involved corrupt payments paid to Mexican foreign officials who had responsibility for maintaining Mexico's aircraft fleet, in violation of the US Foreign Corrupt Practices Act (FCPA). In exchange for the payments (which were made to and from bank accounts in Texas, owned by Hunt Pan

20 US DOJ press release, 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges' (footnote 8, above).

21 US Immigration and Customs Enforcement, news release, 'San Diego Tunnel Task Force Uncovers Sophisticated Cross-Border Drug Tunnel Under the US/Mexico Border' (31 March 2020), at https://ice.gov/news/releases/san-diego-tunnel-task-force-uncovers-sophisticated-cross-border-drug-tunnel-under.

22 Id.

23 Id.

24 Id.

25 Foreign Corrupt Practices Clearinghouse, Stanford Law School, at http://fcpa.stanford.edu/enforcement-action.html?id=643.

© Law Business Research 2021

Am and the government officials), the government officials awarded contracts for aircraft maintenance and parts to Hunt Pan Am.[26]

The US Securities and Exchange Commission (SEC) has likewise pursued cross-border investigations with Mexico, including in a matter using satellite imagery of land in Mexico as evidence against a Mexican company and its employees. In March 2017, the SEC announced that Mexico's largest homebuilder, Desarrolladora Homex SAB de CV (Homex), 'had agreed to settle charges that it reported fake sales of more than 100,000 homes to boost revenues in its financial statements during a three-year period'.[27] Later in 2017, the SEC announced related charges against four of the company's former executives, all Mexican citizens residing in Mexico.[28]

The SEC alleged that Homex improperly recognised billions of dollars of revenue by 'systematically and fraudulently report[ing] revenue from the sale of tens of thousands of homes annually that it had neither built nor sold'.[29] The SEC's complaint contained satellite images of land in the Mexican state of Guanajuato showing 'housing units which Homex claimed to have built or sold, and for which it had recorded sales and reported revenue', but had clearly not been built.[30] Melissa Hodgman, Associate Director of the SEC's Enforcement Division, noted that the SEC 'used high-resolution satellite imagery and other innovative investigative techniques to unearth that tens of thousands of purportedly built-and-sold homes were, in fact, nothing but bare soil'.[31]

Although Homex is based in Mexico, the SEC claimed jurisdiction because the company's stock had been listed on the New York Stock Exchange.[32] In its announcement of the settlement, the SEC noted that it 'appreciates the assistance of the Mexican Comisión Nacional Bancaria y de Valores',[33] a regulatory agency that supervises Mexican financial entities. The Mexican government announced that it carried out the investigation jointly with the SEC and imposed its own penalties against Homex and some of its

26 US DOJ, Justice News, 'Four Businessmen and Two Foreign Officials Plead Guilty in Connection with Bribes Paid to Mexican Aviation Officials' (27 December 2016), at https://www.justice.gov/opa/pr/four-businessmen-and-two-foreign-officials-plead-guilty-connection-bribes-paid-mexican.

27 US Securities and Exchange Commission (SEC), 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (3 March 2017), at https://www.sec.gov/news/pressrelease/2017-60.html.

28 Complaint, *Securities & Exchange Commission v. Gerardo de Nicolas Gutierrez*, Case No. 17 CV 2086 (S. D. Cal. 2017).

29 Complaint, *Securities & Exchange Commission v. Desarrolladora Homex S.A.B. DE C.V.*, Case No. 17 CV 432 (S. D. Cal. 2017).

30 Id.

31 SEC press release, 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (3 March 2017), at https://www.sec.gov/news/pressrelease/2017-60.html.

32 Matt Egan, 'Mexican company faked the building of 100,000 homes: SEC', *CNN Business* (3 March 2017), at https://money.cnn.com/2017/03/03/investing/mexico-homex-fraud-fake-home-sales/index.html.

33 SEC press release, 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (footnote 31, above).

© Law Business Research 2021

officials in addition to the penalties imposed by the SEC.[34] Mexico's National Banking and Securities Commission fined the company US$1.2 million.[35]

Mexico's enhanced corruption enforcement

Mexico has made a concerted effort in recent years to enforce its existing criminal code to combat corruption. President López Obrador, who was elected in 2018, ran on a campaign of taking on the 'mafias of power' and shifting away from what has traditionally been viewed as relatively lax enforcement of Mexico's anti-corruption laws.[36] Following López Obrador's election, the Senate enacted a new law that created a Chief Prosecutorial Office and appointed Alejandro Gertz Manero, a former attorney general of Mexico, to fill the role of chief prosecutor.[37] Gertz Manero announced in May 2019 that his office would begin building criminal corruption cases that had sat dormant in the previous administration.[38] At the time of López Obrador's election, more than 300,000 investigations – a disproportionate number of which related to bribery and corruption of elected officials – had been backlogged.[39]

Thus far, both López Obrador and Gertz Manero have made progress. In March 2019, López Obrador appointed Luz Mijangos Borja as Mexico's first Chief Anti-Corruption Prosecutor.[40] She opened 680 new investigations during her first eight months in office.[41]

In June 2019, the López Obrador administration froze assets and issued arrest warrants in connection with the sale of a fertiliser plant from a state-owned Mexican oil and gas company (Pemex) to one of Mexico's biggest multinational companies (AHMSA).[42] In February 2019, Emilio Lozoya, Pemex's former chief executive officer, was arrested in Spain on corruption charges relating to the sale.[43] He finally agreed to drop his extradition challenge in June 2020 and will return to face charges in Mexico.[44] Lozoya is accused of

34 Government of Mexico, 'Sanctions on the Homex Issuer', at https://www.gob.mx/cnbv/prensa/sanciones-a-la-emisora-homex?idiom=es.

35 Richard Marosi, 'Mexico's Homex faces accusations of massive fraud from the SEC, but the case has stalled', *Los Angeles Times* (2 March 2018), at https://www.latimes.com/world/mexico-americas/la-me-homex-sec-20180302-story.html.

36 Martha Mallory, 'Mexico joins the anti-bribery enforcement bandwagon', *The FCPA Blog* (12 June 2019), at https://www.fcpablog.com/blog/2019/6/13/mexico-joins-the-anti-bribery-enforcement-bandwagon.html.

37 Luis Dantón Martínez Corres, 'Mexico enforcement agencies eye "low hanging fruit"', *The FCPA Blog* (5 March 2019), at https://www.fcpablog.com/blog/2019/3/5/mexico-enforcement-agencies-eye-low-hanging-fruit.html.

38 Brandt Leibe et al., 'H1 2019 Latin American Enforcement Observations', King & Spalding (8 August 2019), at https://www.kslaw.com/blog-posts/h1-2019-latin-america-enforcement-observations-2.

39 '300,000 incomplete investigations, anarchy and extravagant spending in AGO', *Mexico News Daily* (7 May 2019), at https://mexiconewsdaily.com/news/300000-incomplete-investigations/.

40 Luis Dantón Martínez Corres, 'New Corruption Prosecutor Opens 680 Investigations', *The FCPA Blog* (18 December 2019), at fcpablog.com/2019/12/18/new-corruption-prosecutor-opens-680-investigations/.

41 Id.

42 Martha Mallory, 'Mexico joins the anti-bribery enforcement bandwagon' (footnote 36, above).

43 'Ex-chief of Pemex will finally be extradited to Mexico', *The Yucatan Times* (30 June 2020), at https://theyucatantimes.com/2020/06/ex-chief-of-pemex-will-finally-be-extradited-to-mexico/.

44 Id.

© Law Business Research 2021

accepting millions of dollars in bribes and is reportedly co-operating with prosecutors and possibly turning over evidence implicating former president Enrique Peña Nieto in bribes paid for support of his energy reform plan.[45]

Efforts like these may well expand as further progress is made. For instance, in May 2020, the López Obrador administration announced a probe into Leon Manuel Bartlett, son of the head of Mexico's national electricity company (CFE).[46] López Obrador has said that his government will investigate allegations that Manuel Bartlett sold overpriced ventilators to the state arm of Mexico's social security institute during the covid-19 crisis.[47]

Additionally, 18 anti-corruption magistrates are to be appointed to the Federal Tribunal for Administrative Justice, which has exclusive jurisdiction over grave administrative offences such as embezzlement and money laundering.[48] As at April 2020, however, only three individuals had been nominated.[49] Nonetheless, further implementation of Mexico's National Anti-Corruption System – a framework for a tougher and more comprehensive approach to battling corruption – is also planned.[50]

Expansion of Mexico's anti-corruption laws

In August 2019, the Mexican government passed the National Law for Dominion Extinction, which will allow the federal government to transfer ownership of any type of property derived, or presumptively derived, from illegal activities without indemnity or payment to the owner.[51] The country simultaneously expanded the definition of the type of conduct that could trigger asset forfeiture to include corruption, both by corporate entities and public servants as private persons.[52] In March 2020, Mexico's Specialist Bureau for Combating Corruption, part of the Chief Prosecutor's Office, submitted its

45 Mary Beth Sheridan, 'Mexico expects blockbuster corruption case with return of former Pemex chief', *The Washington Post* (16 July 2020), at https://www.washingtonpost.com/world/the_americas/mexico-expects-blockbuster-corruption-case-with-return-of-former-pemex-chief/2020/07/16/02b15e0e-c6d2-11ea-a99f-3bbdffb1af38_story.html/.

46 Raul Cortes, 'Son of Mexican official probed over ventilator sales to government', *Reuters* (4 May 2020), at https://uk.reuters.com/article/uk-health-coronavirus-mexico-corruption/son-of-mexican-official-probed-over-ventilator-sales-to-government-idUKKBN22G2KE/.

47 Id.

48 Gina Hinojosa and Maureen Meyer, 'WOLA Report: The Future of Mexico's National Anti-Corruption System' (7 August 2019), at https://www.wola.org/analysis/report-anticorruption-lopez-obrador-mexico/.

49 Gina Hinojosa and Maureen Meyer, 'WOLA Report: Five Years On, What's Still Missing from Mexico's National Anti-Corruption System' (15 April 2020), at https://wola.org/analysis/five-years-anti-corruption-system-mexico/.

50 Id.

51 Carlos Leo Varelas, 'Compliance Alert: Mexican government grants itself right to seize and sell "unexplained" corporate assets', The FCPA Blog (16 August 2019), at https://www.fcpablog.com/blog/2019/8/16/compliance-alert-mexican-government-grants-itself-right-to-s.html.

52 Luis Dantón Martínez and Juan José Paullada, 'Practice Alert: Mexico expands asset forfeiture to anti-corruption enforcement', *The FCPA Blog* (16 July 2019), at https://www.fcpablog.com/blog/2019/7/16/practice-alert-mexico-expands-asset-forfeiture-to-anti-corru.html.

© Law Business Research 2021

first annual report to the Senate.[53] In it, the Bureau announced its intention to propose modifications to several anti-corruption laws to strengthen prosecutorial power, including amendments to the criminal code, the code of criminal procedure, anti-money laundering law and national asset forfeiture law.[54]

In December 2018, the federal-level Citizen Participation Committee presented a proposal for a National Anti-Corruption Policy, with 60 priority strategies for combating corruption through investigations, awareness, civil involvement and access to public service.[55] The Committee has also advocated for whistleblower protections and greater autonomy for institutions involved in identifying official misconduct.[56]

With the renewed energy and focus on anti-corruption enforcement in Mexico, it is likely that corporations operating in Mexico will begin to face greater scrutiny from Mexican officials. If the current trajectory holds, corporations should expect Mexico to join the United States and Canada as a significant player in corporate anti-corruption efforts.

Co-operation between the United States and Canada

Recent cross-border interactions

Extradition of Meng Wanzhou

The arrest by Canadian authorities of a prominent Chinese national at the behest of the United States has garnered widespread media attention and continues to unfold. Meng Wanzhou, the chief financial officer of Chinese multinational technology company Huawei, deputy chairwoman of the Huawei board and daughter of Huawei's chief executive officer and founder, was arrested at the request of the DOJ on 1 December 2018, at Vancouver International Airport, on multiple federal criminal charges,[57] such as bank fraud, trade secrets theft and sanctions evasion.[58] Meng has been fighting extradition from Canada to the United States since January 2020.[59] A judge dispensed with Meng's

53 Luis Dantón Martínez and Marta Loubet, 'Practice Alert: Mexico's Anti-corruption and compliance developments despite Covid-19', *The FCPA Blog* (17 April 2020), at https://fcpablog.com/2020/04/17/practice-alert-mexicos-anti-corruption-and-compliance-developments-despite-covid-19/.

54 Id.

55 Gina Hinojosa and Maureen Meyer, WOLA Report (August 2019) (footnote 48, above).

56 Andrew Levine, et al., 'Anti-Corruption Enforcement in Mexico: A Possible Turning Point?', Program on Corporate Compliance and Enforcement at New York University School of Law, at https://wp.nyu.edu/compliance_enforcement/2019/08/12/anti-corruption-enforcement-in-mexico-a-possible-turning-point/.

57 Julia Horowitz, 'Huawei CFO Meng Wanzhou arrested in Canada, faces extradition to United States', *CNN Business* (6 December 2018), at https://www.cnn.com/2018/12/05/tech/huawei-cfo-arrested-canada/index.html.

58 In February 2020, the DOJ filed a superseding indictment against Meng, Huawei and four other Huawei subsidiaries, adding a charge of conspiracy to steal trade secrets. DOJ press release, 'Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets' (13 February 2020), at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

59 'Canadian prosecutors say case against Huawei CFO is about fraud, not sanctions', *Reuters* (10 January 2020), at https://reuters.com/article/us-usa-huawei-tech-canada-idUSKBN1Z92D2.

© Law Business Research 2021

latest challenge to the United States' extradition request on 27 May 2020.[60] Meng and her attorneys had argued that she could not be extradited because the conduct alleged by the United States would not be a crime under Canadian law.[61] A judge sitting on Vancouver's Supreme Court, however, found that the key Canadian standard of double criminality, which considers whether the conduct at issue could be considered a crime under Canadian law, was, in fact, met.[62] Nonetheless, the Canadian extradition process involves multiple phases of review and could take several years to complete.[63]

Meng and her attorneys have vigorously disputed the charges, and have said her arrest was politically motivated. Lawyers for Meng also announced that they were suing the Royal Canadian Mounted Police (RCMP), the Canadian Border Services Agency and the Canadian federal government for breaching Meng's constitutional rights during her detention but prior to her arrest.[64] The Canadian court heard her claims over several weeks in autumn 2020 and the extradition hearings are due to be concluded in April 2021. However, a final decision may take longer to reach if appeals are filed.[65]

Canada has faced significant backlash from China as a result of Meng's arrest, including the detention of Michael Kovrig, a former Canadian diplomat, and Michael Spavor, a Canadian businessman, under suspicions of spying and stealing state secrets; Canadian shipments to China of goods worth billions of dollars have also been blocked.[66] In addition, following Meng's arrest, China quickly retried two Canadian citizens, who had been sentenced to jail for drug smuggling, and sentenced both to death. Both individuals are still currently detained in China.[67]

Kinross Gold FCPA enforcement action

Co-operation between the United States and Canada on anti-corruption matters also continues. In March 2018, for example, the SEC announced a settled action against the

60 Amanda Connolly, 'Caving to China's demand to release Meng Wanzhou would put Canadians in danger: Trudeau', *Global News* (25 June 2020), at https://globalnews.ca/news/7106759/justin-trudeau-meng-wanzhou-judicial-interference/.

61 Clare Duffy, 'The case to extradite Huawei CFO Meng Wenzhou from Canada to the United States can continue, judge rules', *CNN Business* (27 May 2020), at https://edition.cnn.com/2020/05/27/tech/huawei-meng-wanzhou-extradition/index.html.

62 Id.

63 Amanda Connolly, 'Caving to China's demand to release Meng Wanzhou' (footnote 60, above).

64 Dan Bilefsky, 'Meng Wanzhou's Cushy Bail is Raising Hackles in Canada', *The New York Times* (4 March 2019), at https://www.nytimes.com/2019/03/04/world/canada/huawei-canada-meng-wanzhou.html.

65 Tessa Vikander and Moira Warburton, 'Canada judge sides with Huawei CFO on some claims but does not dismiss U.S. extradition case', *Reuters* (29 October 2020), at https://www.reuters.com/article/usa-huawei-tech-canada/canada-judge-sides-with-huawei-cfo-on-some-claims-but-does-not-dismiss-u-s-extradition-case-idUSKBN27E1HW.

66 'Meng Wanzhou: Huawei CFO seeks halt to extradition after Trump comments', *The Guardian* (8 May 2019), at https://www.theguardian.com/technology/2019/may/09/meng-wanzhou-huawei-cfo-seeks-halt-to-extradition-after-trump-comments.

67 Rob Gillies, 'Canada's Trudeau rules out releasing Huawei tech executive', *AP News* (25 June 2020), at https://apnews.com/77c5afe68d09a73e50587fff11915ca6/.

© Law Business Research 2021

Canadian corporation Kinross Gold Corporation for FCPA books and records, and internal controls violations 'arising from the company's repeated failure to implement adequate accounting controls of two African subsidiaries'.[68] Kinross Gold had acquired a number of African subsidiaries in 2010 as part of a US$7.1 billion transaction and, according to the SEC, understood at the time that those subsidiaries 'lacked anti-corruption compliance programs and internal accounting controls'. The SEC alleged that, despite this awareness, Kinross Gold failed to implement adequate controls for more than three years, even though multiple internal audits had alerted the company to the control deficiencies.[69] Moreover, the SEC alleged that even after Kinross Gold implemented various internal controls, it failed to maintain them.[70] Without admitting or denying the findings, Kinross agreed to a cease-and-desist order, a penalty of US$950,000 and undertakings to report on its remedial steps for one year.[71] Kinross Gold stated that it received a declination from the DOJ.[72]

Conviction of Robert Barra under Corruption of Foreign Public Officials Act

Canada has recently enhanced enforcement of its own evolving anti-corruption laws. Prosecutions based on Canada's Corruption of Foreign Public Officials Act (CFPOA), the equivalent of the US FCPA, had been rare historically. In 1998, 2004 and 2011, Canada was criticised by the Organisation for Economic Co-operation and Development (OECD) for not meeting its OECD anti-corruption obligations.[73] In 2013, the CFPOA was amended to add a books and records offence, expand jurisdiction based on nationality, and increase the maximum penalty for convicted individuals.[74]

In January 2019, however, following only the second trial under the CFPOA, Robert Barra, a US citizen, was convicted in the Ontario Superior Court of Justice of agreeing to bribe a foreign public official.[75] The convictions in *R v. Barra and Govindia* arose from the same facts as a 2014 case, *R v. Karigar*, the first case in which an individual – Nazir Karigar, a Canadian – was sentenced to imprisonment for an offence under the CFPOA (he was sentenced to three years in jail).[76] Barra, a former executive of the biometrics company

68 SEC press release, 'Kinross Gold Charged With FCPA Violations' (26 March 2018), at https://www.sec.gov/news/press-release/2018-47.

69 Id.

70 Id.

71 Id.

72 Richard L Cassin, 'Canadian gold miner resolves FCPA charges', *The FCPA Blog* (26 March 2018), at https://www.fcpablog.com/blog/2018/3/26/canadian-gold-miner-resolves-fcpa-charges.html.

73 Global Affairs Canada, 'Bribery and corruption' (10 February 2020), at https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/corruption.aspx?lang=eng.

74 Id.

75 Lawrence E Ritchie, et al., 'Canadian prosecutors secure two more convictions in foreign corruption case', *Osler* (24 April 2019), at https://www.osler.com/en/blogs/risk/april-2019/canadian-prosecutors-secure-two-more-convictions-in-foreign-corruption-case.

76 '*R. v. Barra*: A timely but qualified success for Canada's corruption of foreign public officials regime', Dentons (8 March 2019), at https://www.dentons.com/en/insights/articles/2019/march/8/r-v-barra-a-timely-but-qualified-success-for-canadas-corruption-of-foreign-public-officials-regime.

© Law Business Research 2021

Cryptometrics US, was charged in a conspiracy involving bribing various Air India employees, and a number of Indian government officials, to ensure that Cryptometrics was awarded a contract with Air India to instal facial recognition software at airports.[77] The complaint alleged that Barra 'was a co-Chief Executive Officer of Cryptometrics US, which he controlled' and that 'Cryptometrics US provided the required funding for Cryptometrics Canada's operations'.[78]

Shailesh Govindia, an Indian citizen, was also convicted. Govindia argued that he was not subject to the jurisdiction of the Canadian courts because, at the time of his conduct, he was unaware that the Canadian laws would apply to him. The court rejected this argument, finding 'that a Canadian court did have jurisdiction and that there was a substantial connection to Canada' and that Govindia's mistake of law was not a valid argument.[79]

That Canada used the CFPOA to charge a US citizen who was the executive of a US company for offences that occurred at least in part in New York may represent the beginning of a new era for Canadian enforcement of its bribery laws. The DOJ had long been aware of the allegations regarding Cryptometrics – as early as 2007, 'someone called Buddy sent an email to the fraud section of the US DOJ advising that he had information about US citizens paying bribes to foreign officers'.[80] The DOJ assisted the RCMP in the investigative efforts that led to Govindia's conviction in Canada.[81]

Trends in cross-border investigations

Corporate frauds

On 19 September 2018, Canada's Criminal Code was amended to establish a remediation agreement mechanism (the equivalent of a deferred prosecution agreement in the United States), which may signal an increased focus on enforcement of the CFPOA with regard to corporations. This new tool allows voluntary agreements between prosecutors and organisations accused of committing crimes, which the Canadian government hopes will provide an incentive for companies to rectify their wrongdoing, while avoiding some of the negative consequences of a criminal conviction.[82] Canada's Global Affairs department has described the new tool as 'available for use by prosecutorial authorities – at their discretion, in the public interest and in appropriate circumstances'.[83] In a surprise to some, however, the government declined to enter into a remediation agreement with

77 *R v. Barra and Govindia*, 2018 ONSC 57.

78 Id.

79 Govindia was aware, throughout the negotiations, that his meeting was with a Canadian company. *R v. Barra and Govindia*, 2018 ONSC 57.

80 Id.

81 John Bray, 'Paying Bribes: How Not to Win Business', *Forbes* (27 February 2014), at https://www.forbes.com/sites/riskmap/2014/02/27/paying-bribes-how-not-to-win-business/#614f70157e04.

82 Department of Justice Canada, 'Remediation Agreements and Orders to Address Corporate Crime', at https://www.canada.ca/en/department-justice/news/2018/03/remediation-agreements-to-address-corporate-crime.html.

83 Global Affairs Canada, 'Bribery and corruption' (footnote 73, above).

© Law Business Research 2021

SNC-Lavalin, the embattled engineering giant, over foreign bribery charges.[84] The company instead entered a guilty plea in December 2019, agreeing to pay US$213 million in fines and to be subject to a probation period.[85]

Competition protection enforcement in the digital economy

The co-operation between the United States and Canada is not limited to criminal actions and securities enforcement. Co-operation with regard to antitrust and consumer protection matters has evolved into a robust bilateral enforcement regime. Following the August 1995 Agreement between the Government of Canada and the Government of the United States of America Regarding the Application of Their Competition and Deceptive Marketing Practices Laws (the Agreement), the two nations have closely coordinated on common consumer protection matters.[86] The Agreement sets forth seven obligations for each nation:

- notification about enforcement activities in the other's interests;
- co-operation in enforcement and information exchange;
- coordination in enforcement initiatives;
- avoidance of conflicts;
- consultations to resolve concerns regarding the agreement;
- maintenance of confidentiality; and
- use of principles of comity.[87]

Though these obligations had been in effect for more than 20 years, in 2017 both countries recommitted to strengthening North American co-operation in competition law enforcement in the digital economy.[88] Since this agreement, both countries have made strides towards improving antitrust enforcement in the digital space. Canada unveiled a new Digital Charter, designed to maintain a competitive online marketplace, increased fines and penalties to encourage global digital leaders to promote compliance, increased

84 Sam Fry, 'Ethics watchdog finds Trudeau interfered in SNC-Lavalin bribery case', *Global Investigations Review* (15 August 2019), at https://globalinvestigationsreview.com/article/1196382/ethics-watchdog-finds-trudeau-interfered-in-snc-lavalin-bribery-case/.

85 'SNC-Lavalin division pleads guilty to fraud over Libya activities', *BBC News* (18 December 2019), at https://www.bbc.com/news/world-us-canada-50751905/.

86 Government of Canada, 'Agreement between the Government of Canada and the Government of the United States of America on the application of positive comity principles to the enforcement of their competition laws', at https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/01269.html.

87 Debra A Valentine, 'Cross-Border Canada/U.S. Cooperation in Investigations and Enforcement Actions', US Federal Trade Commission (15 April 2000), at https://www.ftc.gov/public-statements/2000/04/cross-border-canadaus-cooperation-investigations-and-enforcement-actions.

88 Government of Canada, 'Competition Bureau reinforces ties with U.S. and Mexican competition authorities' (20 November 2017), at https://www.canada.ca/en/competition-bureau/news/2017/11/competition_bureaureinforcestieswithusandmexicancompetitionautho.htm.

© Law Business Research 2021

global enforcement coordination, and hosted a global summit to discuss competition policy in the digital era.[89]

The US Federal Trade Commission has likewise launched a Technology Task Force, which is dedicated to monitoring competition in US technology markets, and congressional leaders have taken an interest in understanding competition in the digital marketplace.[90]

Given these trends, and the standing agreement between the United States and Canada, it is likely that corporations will see increased co-operation between the two countries on digital antitrust enforcement in the coming years.

89 Dominic Thérien, et al., 'The New Commissioner of Competition Requests Changes to Address Digital Economy Challenges', *Mondaq* (4 June 2019), at https://www.mondaq.com/canada/privacy-protection/816628/the-new-commissioner-of-competition-requests-changes-to-address-digital-economy-challenges.

90 Peter J Levitas, et al., 'Antitrust Scrutiny of High-Tech: What Does it Really Mean?', Arnold & Porter (15 August 2019), at https://www.arnoldporter.com/en/perspectives/publications/2019/08/antitrust-scrutiny-of-hightech.

© Law Business Research 2021

© Law Business Research 2021

Part II

Investigations Country by Country

© Law Business Research 2021

© Law Business Research 2021

5

Argentina

Gustavo Morales Oliver and María Lorena Schiariti[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The *Notebooks* case is the highest-profile continuing investigation for bribery-related crimes. It was initiated in early 2018 and involves various high-ranking current or former public officials and numerous businessmen. The case is already at the trial stage, which is expected to begin soon. This case has also triggered other parallel investigations, including an investigation into cartelisation by the Antitrust Commission.

In addition, convictions in a high-profile money laundering case were ruled in early 2021 and other criminal investigations that involve high-ranking former and current public officials, and certain businessman and corporations, are moving forward.

2 Outline the legal framework for corporate liability in your country.

There are several statutes that establish criminal sanctions for corporations in Argentina, most notably Law No. 27,401 (on corporate criminal liability for bribery-related crimes), which entered into force in March 2018. Corporations can also incur liability, for example, for economic crimes as prescribed in section XIII of the Federal Criminal Code (e.g., money laundering and terrorism financing), or by virtue of a breach of any of the following statutes:

- Customs Code Law No. 22,415;
- Foreign Exchange Criminal Law No. 19,359;

1 Gustavo Morales Oliver and María Lorena Schiariti are partners at Marval O'Farrell Mairal.

© Law Business Research 2021

- Tax Criminal Law No. 27,430; and
- Drug Trafficking Law No. 23,737.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are regulated by the relevant public registry of commerce as well as other government agencies, such as the Argentine tax authority.

Furthermore, depending on the industry, additional regulatory agencies or entities may issue regulations that govern corporations' activities, such as the Argentine Securities Commission for corporations that trade securities, and the Argentine Central Bank for corporations that provide certain financial services or products.

Jurisdiction between the authorities based on their subject matter and competence is allocated by territory.

There are no specific policies or protocols relating to the prosecution of corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In some instances, the law indicates the degree of suspicion to initiate or defer an investigation to another agency. For example, the Anti-Money Laundering Law No. 25,246 establishes that the Argentine financial intelligence unit shall notify the public prosecutor when there are 'sufficient elements of conviction' to determine that an operation under review may indicate a case of money laundering or terrorism financing.

As regards criminal investigation, the mere affirmation of the possible existence of a crime is enough to initiate an investigation. The authorities have the duty to investigate all facts that come to their knowledge and that can constitute a crime under their jurisdiction.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A notice or subpoena may be challenged through a procedural remedy requesting it to be declared null. It may be admissible when the notice or subpoena contains a serious irregularity that prevents the party from promptly complying with the obligations that stem from it.

The most common irregularities that give grounds for challenging a notice or subpoena include that the notice does not contain the court details, the court details are wrong or service of the complaint was carried out in a domicile other than that of the defendant.

If the notice or subpoena is issued by an administrative authority, it must first be challenged before the administrative authority to allow questioning before the courts.

© Law Business Research 2021

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Argentine law allows individuals suspected of participating in certain crimes set forth in Law No. 27,304 to enter into collaboration agreements with the prosecution. Under this regime, suspects and defendants who provide relevant information may obtain a penalty reduction in exchange for their assistance. Once signed, the collaboration agreement must be submitted to the court for approval.

7 What are the top priorities for your country's law enforcement authorities?

The authorities have not made any formal statements that include corporate enforcement actions as one of their priorities.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

There are certain laws and regulations that establish that corporate compliance programmes will be considered for graduating applicable penalties to legal entities. For example, these provisions are established under Articles 304 and 313 of the Federal Criminal Code (penalising money laundering and other crimes against economic and financial order), Law No. 27,430 (establishing the tax criminal regime) and Law No. 27,401 (penalising bribery-related crimes). In particular, the latter establishes that corporate compliance programmes may also be considered when entities seek exemption from or reductions in penalties under Law No. 27,401.

The Argentine Anti-Corruption Office has issued a set of guidelines to help legal entities comply with the provisions of Law No. 27,401 regarding anti-corruption compliance programmes, which shall be appropriate to the risks, size and economic capacity of the legal entity. In addition, the financial intelligence unit has issued several regulations establishing specific requirements for anti-money laundering compliance programmes, which are mandatory for certain entities and individuals subject to the provisions of Anti-Money Laundering Law No. 25,246.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Argentina lacks a comprehensive legal framework addressing cybersecurity issues. However, there are certain resolutions ruling cybersecurity issues that are applicable to

© Law Business Research 2021

the public sector. Technological Standards for the Federal Public Administration were approved by Disposition 5/2019.

Moreover, Regulation No. 1523/2019 (1) approved the definitions of critical infrastructure and critical information infrastructure and the criteria for identification, (2) determined those sectors subject to the Regulation, and (3) included a cybersecurity glossary. In this connection, Regulation No. 829/2019 of the Secretariat of Modernisation approved the National Cybersecurity Strategy applicable to critical infrastructures and created the Cybersecurity Committee.

In the framework of the Federal Cybersecurity Strategy, the Office of the President's Chief of Staff established an Advisory Committee for the Development and Implementation of Secure Applications for the purpose of advising on security principles and best practices in the development, procurement, and implementation of all application software used by federal agencies in Argentina.

The Argentine Data Protection Authority (ADPA) has issued Resolution No. 47/2018, which establishes two sets of recommended security measures for the processing and conservation of personal data with the aim of ensuring the continuous improvement of the administration, planning and control of information security.

Resolution No. 47/2018 entails a change in the approach towards personal data security that follows the principle of accountability, introduced by ADPA in other recent regulations and in line with the European Union's General Data Protection Regulation. Note in particular that, among these recommended measures, Resolution No. 47/2018 lists that security incidents should be notified to ADPA.

In this regard, the Recommendations for the Use of Geolocation Apps, issued by ADPA in April 2020, state that data controllers should adopt the security measures recommended in Resolution No. 47/2018. Likewise, ADPA approved a set of guidelines governing personal data inspection proceedings that mandates inspectors to verify whether data controllers comply with some recommended measures in Resolution No. 47/2018.

Furthermore, in 2021, the National Information Security Incident Response Centre, a specialist government organisation, was created to respond to security incidents. In this connection, public sector entities and jurisdictions, and suppliers that enter into contracts with them, are required to report security incidents within 48 hours of becoming aware of the occurrence or potential occurrence.

Certain industries have their own cybersecurity regulations and standards (e.g., financial institutions are required to report security incidents to the Argentine Central Bank).

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

On 22 November 2017, the Argentine Congress signed the Convention on Cybercrime of the Council of Europe (ETS No. 185) adopted in Budapest, Hungary, on 23 November 2001 (the Budapest Convention).

In 2008, Argentina passed Cybercrime Law No. 26,338 and amended its Criminal Code to include several cybercrimes, modelling them on those contained in the Budapest Convention. Consequently, the new aspects relate to procedural law and international co-operation. Argentina still uses these rules for securing physical evidence for searches in computer systems, which is inefficient from a digital evidence standpoint.

© Law Business Research 2021

Regarding the approach by law enforcement authorities, various federal and local authorities (including prosecutors and police) have created specialist cybercrime units.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Overall, Argentine criminal law is applicable to acts committed in its territory and places under its jurisdiction (e.g., national aircraft and embassies).

The application of local criminal law is extended to acts committed abroad if the effects of those acts are deemed to be produced in the territory of Argentina or places under its jurisdiction.

Likewise, Argentine criminal law applies to offences committed abroad by agents or employees in the exercise of their public functions on behalf of Argentina. Moreover, criminal law applies to bribery of foreign officials committed abroad by Argentine citizens and legal entities domiciled in Argentina.

Argentina has also ratified several treaties that establish universal jurisdiction over serious crimes, such as genocide and torture.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

There are many legal, operative, strategic, technological, communicational and accounting challenges in cross-border investigations that arise in the initial stage and continue throughout the investigatory process. Some of the most important challenges are the protection of the attorney–client privilege and compliance with data privacy and data protection regulation, especially across jurisdictions that have different legal standards of compliance. Thus, valid evidence gathering is one of the key challenges that cross-border investigations face.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Argentine law protects against double jeopardy, that is to say a person who has been convicted or acquitted of an offence cannot be prosecuted again for the same offence.

The principle of double jeopardy (also known as *ne bis in idem*) is established in the Federal Criminal Code, the Federal Constitution and certain human rights treaties that have constitutional hierarchy in Argentina. The law does not distinguish between federal and foreign jurisdictions when it prohibits double jeopardy. Depending on the

© Law Business Research 2021

jurisdictions involved, there may be co-operation treaties establishing rules to resolve a potential double jeopardy conflict.

The fact that a corporation has entered into a deferred prosecution agreement (DPA) in another country is unlikely to prevent prosecution in Argentina, unless a treaty prescribes otherwise or the DPA is viewed as being equivalent to an acquittal, a conviction or any other decision that puts an end to the criminal proceeding.

There is nothing analogous to the 'anti-piling on' policy in the United States between Argentinian law enforcement authorities.

14 Are 'global' settlements common in your country? What are the practical considerations?

There are no relevant 'global' settlements in place involving Argentina as yet, although Argentine enforcement authorities co-operate with foreign authorities, and vice versa.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions made by foreign authorities may attract the attention of Argentine authorities and be the catalyst for local investigations.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Argentina has not implemented a specific autonomous trade sanctions system. However, Argentina complies with the sanctions established in resolutions by the United Nations Security Council (UNSC). Compliance with these sanctions is mandatory for Argentina and for Argentine individuals and legal entities, provided that the Ministry of Foreign Affairs has published the UNSC's resolutions in the Argentine *Official Gazette*.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Argentina has not conducted any relevant enforcement activity.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Argentina has not conducted any relevant enforcement activity.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Law No. 24,871 regulates the extent of the application of foreign regulations. In particular, it sets forth that any foreign laws establishing extraterritorial sanctions intended to trigger, for example, negative consequences on a third country would be deemed null and inapplicable in Argentina.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Any individual or legal entity shall invoke rights, execute or claim the execution of acts or be compelled to comply with measures, orders, instructions or indications that are a consequence of the extraterritorial application of foreign regulations to the extent stipulated in Law No. 24,871.

Furthermore, Law No. 24,871 establishes additional provisions regarding, for example, the enforcement of foreign rulings under the aforementioned foreign regulations, or the exchange of information between Argentine authorities and the authorities of the foreign country issuing sanctions.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

In our experience, most allegations of wrongdoing within companies in Argentina have been made through whistleblower hotlines. Also, as practitioners in this field, we have noticed that local companies are increasing their awareness of and attention to corporate internal investigations.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Personal data protection is governed by Personal Data Protection Law No. 25,326 (PDPL), of which the main purposes are guaranteeing (1) the complete protection of the data contained in files, records, databases or other technical means, whether public or private, and (2) the rights to reputation, privacy and access to information. Any information relating to individuals or companies, whether identified or identifiable, is considered personal data and subject to the terms of the PDPL.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The PDPL is enforced by the Argentina Data Protection Authority and the judicial courts. Depending on the type of behaviour, failure to comply with the PDPL could be considered a minor, serious or very serious infringement. At the same time, data subjects

© Law Business Research 2021

could file court action seeking the cessation of processing of their data and compensation for damage caused, including the possibility of filing class actions.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

As a general rule, valid data processing requires the free, express, informed and written (or similar) consent of the data subject (i.e., the relevant individual or legal entity). Data subjects are free to revoke their consent, although this will only have effect for the future (not retrospectively). They also have the right to have access to, rectify and delete their personal data. Treatment of data that is limited to the data subject's name, identification number, tax identification number, occupation, date of birth and domicile does not require consent.

Moreover, the PDPL determines restrictions to cross-border transfers of data.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

From a privacy perspective, it is highly important to provide employees with prior notice and an explanation of the way in which the company processes data (generally through corporate information technology or privacy policies).

From a labour law perspective, there are no specific regulations in force regarding the access, monitoring and surveillance of electronic communications and devices in the workplace. Although there is case law on this issue, it is not uniform.

It is of key importance to analyse any internal policy (duly notified to the employees) relating to the monitoring of corporate emails and, upon default thereof, implement an internal policy for the monitoring of emails, other electronic communications and devices, and the use of working tools and to notify employees in advance that (1) electronic communications and devices are work tools and, thus, they shall be used only for work purposes, and (2) they should have no expectation of privacy in connection with their use (even if a personal password has been created). Further, a company should have in place further provisions for monitoring employees' activity and, ultimately, to prove misconduct.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

According to the Argentine Criminal Procedural Code, if there is reason to presume that in a certain place there are things of relevance to the investigation of a crime, or the suspicion of a criminal offence, a judge may issue a search warrant. Further, a judge may order the seizure of objects and documentation that (1) may be relevant to the investigation, (2) may be subject to confiscation or (3) can serve as evidence.

© Law Business Research 2021

Besides the formal requirements, search warrants must indicate the crime under investigation, the exact place where the search will be conducted and its purpose. If any of these requirements are not fulfilled, the search – and any evidence collected during the search – can be challenged in court.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The Argentine Criminal Procedural Code protects letters and documents sent to or received by a defendant's counsel from being seized, as long as they are connected to a criminal investigation.

Moreover, a judge may request the testimony of witnesses and third parties and the submission of documents in their possession. However, this order shall not be addressed to persons exempted from testifying as witnesses by reason of family or professional links, or state secrecy.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Judges can request the testimony of any person who may have relevant information relating to a criminal investigation. The request is mandatory and the person summoned to render testimony must appear before the judge and state the truth of what they know, unless an exception applies. Failure to do so may be construed as contempt of court or harbouring, and may trigger raids to seize the information. According to Argentine law, these offences are only attributable to individuals.

Argentine law protects the right against self-incrimination. For instance, when a representative of a legal entity is called to provide information relating to a criminal investigation, the representative may refuse to give testimony on the basis of the constitutional right against self-incrimination.

Additionally, the Argentine Criminal Procedural Code establishes that those who must keep the secrecy of whatever they learn by virtue of their service, profession or official capacity must abstain from rendering testimony of facts and issues covered by that secrecy. This expressly applies to lawyers, notaries, doctors, nurses, military personnel and public officials, among others. However, they cannot refuse to give testimony when released from their secrecy duty by the interested party.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Law No. 27,319 regulates special techniques that can be used in the investigation of certain complex crimes, such as those relating to drugs, smuggling, terrorism and economic matters.

© Law Business Research 2021

Under this framework, persons who provide useful and relevant information to initiate or guide an investigation concerning the crimes set forth in Law No. 27,319 will be entitled to receive financial compensation. The identity of whistleblowers will be withheld and, if necessary, other adequate measures may be ordered to protect the life and integrity of the whistleblower and his or her family.

Additionally, Emergency Decree 62/2019 establishes a financial reward for those persons – whose identity is preserved – that provide useful information within civil asset forfeiture procedures triggered by certain crimes (e.g., corruption-related crimes).

Depending on the circumstances, other regimes may apply. For instance, a permanent rewards fund for whistleblowers was used to offer monetary rewards in exchange for useful information to trace and recover assets in the *Notebooks* case.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There is no specific labour regulation regarding investigations or a specific procedure for internal investigations. Nevertheless, labour and civil rights are fully applicable to all employees. Thus, any kind of discrimination or adverse effect on employees' dignity or right of defence could be challenged within the context of an investigation.

Investigations should be carried out as quickly as possible, so that disciplinary action, if any, can be decided as soon as possible after discovery of the behaviour under investigation.

If the personnel involved are board members or authorised signatories of a company, measures regarding removal of control and replacement to ensure the normal operation of the company should be analysed jointly.

Furthermore, since each case will be different on its merits, there could be different practical matters to consider within the context of a labour investigation; thus, it is important to duly liaise with the appropriate legal adviser.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Different courses of action and different sanctions could be implemented, depending on the seriousness of the misconduct, the extent to which it affects an employer's activity or business, the level of responsibility of the relevant employee and previous performance, among other things. These aspects should be considered in each particular case.

Damage caused by the misconduct could also be considered, although this is not essential since the misconduct itself could be subject to disciplinary measures. Possible sanctions could involve a first warning, suspension from duty without payment of salary or even dismissal with just cause, subject to full analysis of the case in question.

Prior to implementing any course of action or disciplinary sanction, it is important to consider that (1) there are both specific requirements applicable to disciplinary sanctions

© Law Business Research 2021

and practical legal recommendations, and (2) dismissal with just cause is interpreted narrowly in Argentina.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Employees are entitled to refuse to participate in an internal investigation, without their refusal construing a just cause for termination of the employment contract.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Before commencing an internal investigation, it is useful for companies to draft a flexible investigation plan, which may lead the investigation process and determine, among other things, its scope, time limits and main objectives.

There is currently no legal requirement for an investigation plan. Therefore, in practice, implementing such a plan depends on each company, the complexity of the subject under investigation and the regulations involved.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Law No. 27,401 (on corporate criminal liability for bribery-related crimes) addresses the concept of internal investigations and sets forth that each legal entity, depending on the risks to its activities, may implement an internal investigation system.

In general, there is no particular legal obligation to comply when misconduct is discovered during an internal investigation. However, certain industry-specific regulations may establish additional provisions regarding internal investigations, which companies should consider.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

If a company receives a notice seeking the production of documentation or a subpoena requiring its testimony to clarify the facts or allegations under investigation, the company shall comply within the terms specified, unless it is subject to any exception provided in the applicable regulation.

There is no specific regulation setting forth mandatory steps for companies to comply with such notices or subpoenas. Therefore, the measures implemented may depend on the company's policies and procedures, the facts and persons under investigation, and so on.

© Law Business Research 2021

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

A public company in Argentina is not obliged to disclose the existence of an internal investigation until the investigation results in verification of the existence of an event that, in all likelihood, could have a substantial effect on the company's trading value (except when an investigation was commenced following verification of the existence of an event having such effects, which must be disclosed). Likewise, there is no obligation to disclose any contact by a law enforcement authority until the company is served with notice of the commencement of formal proceedings (except where the circumstances are made public or disclosure is required by a law enforcement authority).

37 How are internal investigations viewed by local enforcement bodies in your country?

Provided that the rights of employees are respected, internal investigations are tolerated. Investigations of wrongdoings and crimes in Argentina are usually conducted by law enforcement authorities; therefore, as yet, acceptance among local agencies is not widespread.

Law No. 27,401 (on corporate criminal liability for bribery-related crimes) encourages companies to implement an internal investigation system that respects the rights of investigated persons and allows the imposition of sanctions on those who breach a company's policies.

In this sense, an internal investigation may be useful to show the authorities that the company acted diligently and in good faith to try to identify and remedy potential misconduct or wrongdoing. So far, there are no precedents under Law No. 27,401 to establish how law enforcement agencies will assess the efforts taken by companies during an internal investigation.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

The attorney–client privilege stems from the constitutional right to defence during trial and privacy. The Federal Criminal Code and certain procedure codes prohibit disclosure of protected confidential information when obtained or produced by attorneys, unless certain specific exceptions apply. Also, there are laws and regulations governing the exercise of legal practice that provide that the attorney–client privilege is both a right and a duty that attorneys must observe, other than in specific circumstances (e.g., their personal defence).

© Law Business Research 2021

There is very little legislation in Argentina regarding the attorney–client privilege, nor is there any jurisprudence on the matter since this kind of protection is not often raised with or discussed before the courts. Thus, to protect the privilege of an internal investigation, it is recommended that international best practices are followed (e.g., marking documents as confidential and protected by the attorney–client privilege).

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The aim of the attorney–client privilege is to protect communications and information exchanged in private between an attorney and a client (legal entity or individual) for the purpose of the attorney providing legal advice. In any case, the client may waive the privilege since it is the holder of the privilege. The attorney has the duty and the right to protect the privileged information.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The applicable regulations do not make a distinction between in-house and external counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

This is a situation that is not regulated and, to our knowledge, has not been tested with the local courts yet.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There are no precedents that would allow us to consider waiver of the attorney–client privilege as a co-operative step. Privilege waiver is not mandatory or required.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The applicable regulations do not stipulate partial waivers.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This is a situation that, to our knowledge, has not been tested with the local courts yet.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept does not exist in Argentina.

© Law Business Research 2021

46 Can privilege be claimed over the assistance given by third parties to lawyers?

This is a situation that, to our knowledge, has not been tested in the local courts yet.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Witness interviews as part of internal investigations in Argentina are not forbidden or specifically regulated.

Nonetheless, guidelines issued by the Argentine Anti-Corruption Office briefly address certain mechanisms for corporate investigations, including witness interviews. In particular, these guidelines emphasise that all the investigative mechanisms carried out by companies shall not put the rights of employees in jeopardy.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

There is no law that particularly regulates the extent of the attorney–client privilege in internal investigations. In this context, a company may claim the attorney–client privilege over internal witness interviews or attorney reports, but the chances of success will depend on the factors relevant to the case.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There is neither Argentine regulation nor relevant judicial precedents setting forth legal or ethical requirements or guidance for conducting witness interviews, whether they involve employee or third parties (e.g., former employees or contractors).

We advise our clients to apply internationally accepted common practices, such as providing *Upjohn* warnings to interviewees, avoiding recording interviews, and preparing reports that merely include attorneys' impressions of the topics addressed in interviews.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The timing, order and steps taken in each interview (e.g., putting documents to the witness) will vary from case to case.

We advise our clients to consider all factors and good practices when carrying out interviews, such as providing *Upjohn* warnings to interviewees, avoiding recording interviews, and preparing reports that merely include attorneys' impressions of the topics addressed. Some case precedents acknowledge, for example, the right of witnesses to be informed about the scope and nature of an interview, and to be accompanied at the interview by their own lawyer.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Under Argentine law, there is no general obligation for individuals or entities in the private sector to report misconduct to law enforcement authorities. However, depending on the industry, some laws and regulations may mandate disclosure of misconduct to the authorities.

Nonetheless, Argentine public officials (a broad definition that includes directors of state-owned companies, etc.) have a duty to report offences of which they become aware in the exercise of their office.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

In general, a company self-reports if it is likely to receive significant leniency from the authorities. For example, Law No. 27,401 (on corporate criminal liability for bribery-related crimes) provides a regime under which companies may seek exemption from criminal and administrative liability arising from self-reporting.

Notwithstanding, self-reporting in Argentina is still unusual. Whether this is a convenient course of action will depend on the specifics of the case (i.e., the facts, regulations and jurisdictions involved).

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Companies may obtain an exemption from criminal and administrative liability under Law No. 27,401 if they (1) spontaneously self-report a breach of the Law to the authorities as a result of an internal investigation, (2) had implemented a compliance programme before the breach occurred and the wrongdoers had to make material efforts to evade controls under the programme, and (3) forfeit the undue benefit arising from the illegal conduct. Practical steps will vary, depending on the specifics of the case, to comply with the requirements of the regulation.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

A company must respond to a judicial notice or subpoena through judicial channels within the relevant legal terms laid down under the Procedure Code.

© Law Business Research 2021

It is possible to enter into dialogue with the authorities to establish the position of the defendants. However, official challenges, requests and decisions must be made through judicial or administrative channels, according to the relevant procedural rules.

55 Are ongoing authority investigations subject to challenge before the courts?

Any decision issued by the centralised or decentralised federal administration is deemed legitimate, but could be challenged before the courts if the requirements set forth in the applicable administrative procedural regulations are fulfilled.

Since Argentina is a federal country, depending on the territorial competence of the relevant authorities, local regulations may be applicable, and the particular requirements established therein shall be considered.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

There is no general statute covering this matter. The approach will have to be assessed for each case, taking into account any applicable laws and international treaties.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

A company must comply with the requirement for production of material relating to a particular matter that crosses borders. However, according to the Federal Civil and Commercial Procedural Code, it is necessary to establish whether the company in question is a party to the proceeding.

In the case of companies acting as plaintiffs or defendants, they must produce the required material (documents or information) that is in their possession, even when the documents or information are outside the country.

If a company is a third party to the proceeding in which the requirement is made, it is also obliged to produce the documents or provide the required information. However, the requested party may challenge the request if the material required is its exclusive property and its disclosure may cause damage.

A company that intends to produce material that is abroad will face certain difficulties that could delay the proceeding. For instance, the company must comply with the requirements imposed by international treaties to verify the authenticity of foreign documents (e.g., through the Hague Apostille or authentication through diplomatic channels as well as translations, among other things). Further, the attendant costs could be significantly higher.

© Law Business Research 2021

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The frequency of co-operation and challenges to co-operation vary according to the law enforcement authorities involved.

On the one hand, in respect of judges and prosecutors, cross-border co-operation and exchanges of information usually proceed after a long time because of the many difficulties that can arise. For instance, according to press articles, Argentine authorities were provided with leniency agreements and evidence produced in the *Operation Car Wash* bribery investigation in Brazil only four years after its initial request.

On the other hand, certain law enforcement authorities most often share information within the federal administration. For example, the Argentine financial intelligence unit – being a member of the Egmont Group of Financial Intelligence Units – shares information with other units across the world, and the Argentine tax authority shares information in accordance with the Common Reporting Standard, among other methods.

Furthermore, international treaties (whether multinational or bilateral) may govern cross-border co-operation.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Overall, law enforcement authorities are bound to maintain confidentiality with respect to information obtained during investigations. They shall not share or disclose information or documents unless the conduct falls within one of the exceptions set forth in their statutes or applicable laws.

In some cases, the law allows the transfer of information between law enforcement agencies. For instance, the Argentine tax authority may share certain information with revenue agencies from the provinces, or foreign tax agencies, in accordance with applicable co-operation agreements.

In the course of a criminal investigation, the secrecy of the proceedings shall be respected. In particular, under Law No. 27,401 (on corporate criminal liability for bribery-related crimes), when corporations enter into negotiations with the prosecution with the aim of concluding a collaboration agreement, the information shared during the negotiation will be kept confidential.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In these circumstances, companies should claim an exemption and inform the relevant law enforcement authority that they cannot reasonably comply with the request without violating the laws of another country.

© Law Business Research 2021

In addition, foreign legal advice should be obtained as to the company's exposure to liability if it produces the requested information.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Certain statutes and regulations set forth secrecy obligations, including those relating to banking (Law No. 21,526), tax (Law No. 11,683), certain professions (e.g., attorneys, physicians) and confidential commercial information (Law No. 24,766). These statutes and certain regulations (e.g., Anti-Money Laundering Law No. 25,246) establish certain circumstances when secrecy does not prevail and compliance with a notice or subpoena becomes mandatory.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The rules applicable in a certain jurisdiction and the type of proceeding initiated against a company will determine the applicable rules of evidence. Nonetheless, Argentina does not regulate discovery rules. Thus, production is compelled by law enforcement authorities and interested parties can occasionally produce complementary evidence (e.g., expert witnesses).

Production of evidence within civil procedures is usually available to the parties and any other stakeholder, unless confidentiality is expressly imposed, which may be the case, for instance, in procedures where family issues are in question or when minors are involved.

Production of evidence within criminal procedures is often confidential and withheld from the parties (including private prosecutors) during the investigative stage. However, during the trial stage, production of evidence is, in general, not subject to confidentiality and is accessible by the general public.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies may be subject to the following penalties:

- fines that normally will be determined based on the 'undue' benefit obtained or that could have been obtained through the crime;
- total or partial suspension of activities;
- debarment from participating in government bids and contracts, or in any other activity relating to the government;
- dissolution and liquidation of the legal entity;
- suspension or termination of government benefits;
- publication of the conviction sentence at the cost of the convicted entity; and
- forfeiture of assets obtained through the illegal actions.

© Law Business Research 2021

Directors, officers and employees are subject to the penalties prescribed for the specific crime in the relevant statutes. Penalties for individuals include imprisonment, fines and debarment. Additionally, defendants may be subject to forfeiture of assets that have been obtained illegally.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Depending on the circumstances (such as the existence of a criminal investigation or whether precautionary measures were issued against the company), there might be restrictions on relocating assets sited or registered in Argentina to another country.

65 What do the authorities in your country take into account when fixing penalties?

In a criminal trial, judges must refer to the penalty scale for the crimes and take into account aggravating and mitigating circumstances, whenever applicable. Additionally, they will consider, among other things:

- the nature of the conduct;
- the means employed to commit the crime;
- the injury or risks caused;
- the personal circumstances of the defendant, such as age and education;
- conduct during the proceedings;
- the motive to commit the crime (especially state of necessity or indigence);
- the degree of participation in the crime; and
- recidivism.

Moreover, in respect of economic and financial crimes committed with intervention, on behalf, or for the benefit, of a legal entity, judges will also consider:

- compliance with internal rules and procedures;
- failure to monitor the conduct of the perpetrators and accomplices;
- the extent of the damage caused;
- the amounts of money involved;
- the size, nature and economic capacity of the legal entity; and
- the need to continue the activities of the company (for the purposes of suspension or debarment).

Finally, in respect of publicly traded companies, penalties shall be prescribed having in mind the protection of shareholders to whom no liability is attributable.

© Law Business Research 2021

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Since the enactment of Law No. 27,401 (on corporate criminal liability for bribery-related crimes), corporations can enter into 'effective collaboration agreements' with the prosecution to obtain a reduction of applicable penalties. To this end, companies must disclose precise and verifiable information that is useful for the investigation. The agreement is subject to court approval to enter into effect. So far, there are no precedents of collaboration agreements signed by corporations.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

In respect of effective collaboration agreements under Law No. 27,401 (on corporate criminal liability for bribery-related crimes), all negotiations are deemed to be strictly confidential until the conclusion of an agreement with the public prosecutor.

Law No. 27,401 makes no reference to the confidentiality of the information after the agreement is concluded and approved by the criminal judge. Therefore, there are no provisions that determine reporting restrictions or anonymity until the conclusion of the criminal proceedings. In a particular case, specific consideration may be given to confidentiality depending on the potential risks that may affect a fair resolution of proceedings.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

When considering entering into an agreement with any Argentine enforcement authority, a company should conduct a thorough analysis of the alleged facts and the possible legal violations that may be triggered, either in Argentina or abroad. The company should also consider whether entering into a collaboration agreement would allow the authorities to gather information to prosecute other crimes.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Corporate compliance monitors are not regulated as an enforcement tool in Argentine law.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

When criminal conduct gives rise to civil liability, Argentine law allows both civil and criminal actions to be pursued simultaneously. Both proceedings are independent of each other; however, the civil judge is foreclosed from reaching a decision until a judgment is

© Law Business Research 2021

passed on the criminal case. Therefore, plaintiffs usually do not incur effort and expenses until a decision is reached by the criminal court.

In criminal cases, the Argentine Criminal Procedure Code recognises victims' right to offer and control evidence. It prescribes that the case docket is public to the parties, which includes the private prosecutor but not the civil petitioner, whose participation is limited to claiming compensation, restitution or other civil remedies. Despite this general principle, during a criminal investigation, judges may be reluctant to grant private prosecutors full access to some confidential information for reasons of security or privacy. During the trial, the private prosecutor has access to all files and evidence that will be used in court.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In criminal investigations governed by the Argentine Criminal Procedure Code, the docket file is withheld until the first appearance of the defendant before the judge (the investigative statement), where the defendant is put on notice about the investigation and informed of his or her rights.

However, third parties (e.g., the defendant, the victim and state authorities) may request information if they justify having a 'legitimate interest'. After this stage, the docket file can be accessed by the parties, including the defendant, the public prosecutor and the private prosecutor, if any. Notwithstanding the foregoing, judges may order the secrecy of some information when disclosure would jeopardise the investigation. Only acts that cannot be reproduced at a subsequent stage shall not be kept confidential. The docket file will continue to be withheld from third parties during the investigation.

Once the case is at trial, hearings are public unless the court decides, as an exception, to limit access by some or all public parties (e.g., relevant witnesses who have not yet given their testimony).

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In our experience, companies have used both their in-house public communications department and external firms. Larger companies are more likely to retain the services of public relations companies when there is a risk of negative publicity.

73 How is publicity managed when there are ongoing related proceedings?

First, it should be assessed whether there are any disclosure restrictions. Then, public communications, whether involving an external public relations company or not, should be vetted by the company's legal adviser and the team in charge of litigation to ensure that there is nothing that could compromise the company's position in the proceedings.

© Law Business Research 2021

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Settlements made within a criminal action must be disclosed upon service of process. Disclosure of settlements is forbidden until endorsement by the criminal court, and breach of confidentiality obligations is subject to sanctions under the Federal Criminal Code.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

There are specific industry guidelines and guidelines applicable to companies whose equity is totally or partially owned by the government that address ESG matters. For example, ESG matters are covered in the Corporate Governance Code proposed by the Argentine Securities Commission in an attempt to meet the international standards set forth by the Organisation for Economic Co-operation and Development. Although implementation of this Code is not mandatory, organisations are required to provide explanations if they do not implement the Code and its recommendations (comply or explain).

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

In recent years, certain guidelines have been issued as a result of an increase in awareness of ESG matters. However, these matters are not regarded as a top priority for the current government's agenda.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

We are not aware of specific enforcement actions triggered by ESG matters. However, judicial cases may be triggered when conduct that breaches ESG guidelines also involves violation of an applicable law.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Certain bills that address corporate misconduct, asset recovery and corruption-related crimes have been introduced to the Argentine Congress, including a new bill to reform the Criminal Code. Considering the most recent decisions by the Argentine government, specific emphasis is expected in preventive measures rather than enforcement actions for misconduct.

© Law Business Research 2021

6

Australia

Tim Grave and Lara Gotti[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Inquiries into licensing suitability and the regulatory framework in the gaming industry have dominated headlines in 2021, bringing with them allegations of money laundering and poor governance. An independent inquiry in New South Wales was followed by Royal Commissions in Western Australia and Victoria, along with a multi-jurisdictional investigation by the Australian Transaction Reports and Analysis Centre (AUSTRAC) into all of Australia's major casino operators.

The broadening focus emphasises that key regulatory concerns for Australian regulators are now heavily focused on due diligence, the adequacy of compliance frameworks and money laundering accountability with AUSTRAC, noting the link between these areas and organised crime groups or national security interests.

2 Outline the legal framework for corporate liability in your country.

Under Australian law, offences committed by 'a person' will, unless specifically excluded, include a corporation (including those offences punishable by imprisonment). At a federal level, criminal liability is generally established if both physical and fault elements are proven. Fault elements include intention, knowledge, recklessness and negligence. In the case of strict or absolute liability offences, there are exceptions to the proof of fault elements. These offences are more commonly pursued against a corporation.

1 Tim Grave is a partner and Lara Gotti is a senior associate at Clifford Chance. The authors thank their colleague, Kirsten Scott, for her contribution to this chapter.

© Law Business Research 2021

If a fault element is required to be proved against a corporation, it may be shown in a variety of statutorily defined ways, including by proof that a corporation failed to maintain a corporate culture of compliance.

State and territory law equivalents exist in a variety of legislative forms.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Regulation of Australian companies is principally done at federal level, with some limited involvement by state and territory regulators primarily relating to fraud, theft or private sector bribery. There is a broad range of law enforcement agencies that have authority to investigate corporations, including, but not limited to, the following:

- Australian Securities and Investments Commission (ASIC), an independent statutory body that enforces and administers the Corporations Act 2001 (Cth), which is the main corporations legislation in Australia;
- Australian Prudential Regulatory Authority (APRA), a statutory body that supervises the banking, insurance and superannuation bodies;
- Australian Competition and Consumer Commission (ACCC), which regulates the interaction between consumers and businesses;
- Australian Criminal Intelligence Commission, which investigates national serious and organised crime, such as cybercrime;
- Australian Federal Police (AFP), which investigates and enforces cross-border crime, including fraud, drug trafficking, organised crime, money laundering, foreign bribery and corruption, and people smuggling;
- Australian Taxation Office, which enforces compliance with Australia's taxation legislation;
- AUSTRAC, which regulates and enforces cross-border financial transactions; and
- Commonwealth Director of Public Prosecutions, which prosecutes federal criminal misconduct based on referrals from investigatory bodies.

Australian regulatory bodies generally coordinate their efforts so as to share information and intelligence-gathering powers (subject to certain restrictions). In the event of serious criminal allegations, it is common for two or more regulatory authorities to be involved. For example, search warrants executed by the AFP may be attended by members of ASIC in the case of corporate crime allegations. Joint task forces, such as the Serious Financial Crime Taskforce housed with the AFP, have been established to streamline and consolidate information sharing, investigation and reporting lines in Australia.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Regulators have wide-ranging statutory investigatory powers. The trigger point is generally suspicion of a breach of legislation within a regulator's jurisdiction. For example, an investigation under section 13 of the ASIC Act 2001 (Cth) will be commenced if ASIC thinks it expedient for the due administration of corporation legislation and when it has

© Law Business Research 2021

reason to suspect that a contravention may have been committed. The degree of suspicion is not defined but, generally, the threshold is low.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A company should carefully consider the scope of a notice or subpoena and any grounds for objecting to it, including whether it has been properly issued, the information sought is clearly defined and relevant, and the request is not oppressive or unreasonable particularly in relation to time for compliance. Any concerns should be raised directly with the law enforcement authority to ascertain whether clarity or revision of the notice is appropriate. Otherwise, parties can make an application to the court to set aside the notice or subpoena. Challenges to the issue of certain notices, such as search warrants, are often more difficult to achieve as the basis for their issue cannot be readily ascertained with authorities generally claiming public interest immunity over this information.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Australian regulators have significantly changed their approach to immunity and leniency in recent years. In addition to the traditional prosecution policy indemnity applications, regulators such as the ACCC and ASIC have adopted immunity policies to formally confer a benefit to those who wish to co-operate with authorities. The ACCC has a 'first past the post'-style policy that provides immunity to the individual or corporation who is first to disclose cartel conduct and co-operate fully with the investigation. In 2021, ASIC made an immunity policy available to individuals (not corporations) involved in market misconduct, providing immunity from criminal prosecution and civil penalties.

As to leniency, sentencing for criminal conduct is entirely at the discretion of the court. The High Court's decision in *Barbaro v. The Queen* made it clear that a prosecuting body cannot make submissions to the court regarding a preferred sentence or penalty range. More flexibility is provided for negotiated outcomes in civil penalty proceedings.

ASIC issued an Information Sheet (INFO172) in February 2021 outlining the benefits of co-operation, and its approach is similar to other federal agencies.

7 What are the top priorities for your country's law enforcement authorities?

AUSTRAC has emerged as a key law enforcement agency in recent years, with Australian regulators focused clearly on money laundering and corporate governance systems and compliance. Covid-19 lockdowns have contributed to this as an increasing risk. Other areas linked to covid-19 issues are likely to include consideration of both cryptocurrency and 'buy now, pay later' regulation limitations.

The fallout from the Financial Services Royal Commission can still be seen in an increased focus on corporate culture, including executive accountability.

© Law Business Research 2021

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

A number of enforcement authorities provide guidance to companies regarding compliance programmes, including ASIC, the Australian Securities Exchange (ASX) and the AFP. Guidance is publicly available via regulator websites, examples including the 'ASX Corporate Governance Principles and Recommendations' and ASIC's 'Director and officer oversight of non-financial risk report'. Further guidance can also be found in recent enforceable undertakings entered into between APRA and corporate entities as a result of concerns about weaknesses in risk culture, risk governance and risk management.

Specific guidance on aspects of compliance programmes can be found in regulatory policies, such as for credit licensees or those who need to have compliant whistleblowing policies.

The introduction of new legislation, including an offence of failing to prevent foreign bribery and a corresponding defence that adequate procedures are in place, will further necessitate a comprehensive compliance programme. Comprehensive guidance will be provided by the Attorney General's Department as to what this programme looks like.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Cybersecurity is legislated at both federal level and state and territory level through various legislative frameworks relating specifically to cybersecurity and more broadly to data protection and privacy. The Australian Cyber Security Centre (ACSC) leads Australian efforts to improve cybersecurity and sits within the Australian Signals Directorate. To further these efforts, the Joint Cyber Security Centre, established by the ACSC, brings together business, government, academia and other key partners. Cybersecurity incidents are reportable to the ACSC.

The Office of the Australian Information Commissioner (OAIC) regulates privacy and freedom of information. Suspected or actual data breaches involving personal information as a result of cybersecurity incidents are reportable in certain instances to the OAIC under the Notifiable Data Breaches Scheme.

In March 2019, the Australian government announced an intention to increase penalties under the Privacy Act 1988 (Cth) (the Privacy Act) from A$2.1 million to A$10 million or 10 per cent of the company's annual domestic turnover, expand the OAIC's scope to ensure breaches are addressed and add further protections to certain vulnerable groups. Delay in implementing these amendments has been attributed to the government's current focus on responding to the covid-19 pandemic.

For entities regulated by the Australian Prudential Regulatory Authority (APRA), obligations can be found in Prudential Standard CPS 234, which states that notification

© Law Business Research 2021

of an 'information security incident' must be no later than 72 hours after the incident has been discovered. Further, an entity must notify APRA within 10 business days of becoming aware of a 'material information security control weakness' that the entity is unable to rectify.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Legislation provides regulation for computer-related and internet-related offences, such as unlawful access and computer trespass, and creates investigation powers and criminal offences designed to protect security, reliability and integrity of computer data and electronic communication. New federal legislation, the Online Safety Act 2021 (Cth), was introduced in July 2021 and introduces an adult cyber abuse system that removed content posted with the likely intention of causing serious harm. The Act also enhances child cyberbullying protections and the process of removing abusive imagery from the internet.

Since March 2013, Australia has been a member of the Council of Europe Convention on Cybercrime, which addresses both domestic and international responses to cybercrime.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law generally has extraterritorial effect, provided there is an appropriate nexus to Australia. Conduct must have been either wholly or partly undertaken within Australia. Foreign entities who do business in Australia, or who have Australian subsidiaries or associated entities, will fall within Australian laws as regards conduct in Australia. For example, if a foreign entity is conducting business in Australia through a subsidiary and the subsidiary breaches Australia's laws, both might possibly be charged (depending on the applicable facts); for example, the subsidiary for a breach of domestic laws and the foreign entity for directly breaching domestic laws or aiding and abetting the breach.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Australia has entered into mutual assistance treaties with numerous countries in a bid to facilitate information sharing and to expedite investigations. There are also information-sharing arrangements with certain jurisdictions, and therefore a formal request for mutual assistance is not always required. Examples include tax information exchange agreements, agreements forged under the international foreign bribery taskforce and the coordinated approach named 'Five Eyes', which includes Australia, Canada, New Zealand, the United Kingdom and the United States. However, challenges arise when there are inconsistent approaches to an investigation by regulators. Legislative requirements as to the limitations on gathering or sharing of evidence, the integrity of investigators and the reliance on compulsory powers can present issues in cross-border matters.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

A person or corporation cannot be tried twice for the same alleged breach of Australian legislation. There is no prohibition in Australia against being prosecuted by multiple authorities where alleged contraventions of the law span the jurisdiction of multiple regulatory agencies; however, there is usually coordination between jurisdictions and agencies, to ensure prosecutions remain in the public interest.

Double jeopardy does not apply internationally. If offending has traversed multiple jurisdictions, a defendant can be charged with an offence under Australian legislation despite having concluded proceedings of a similar nature in another country. A guilty plea or a negotiated outcome in another jurisdiction, however, may affect the investigation, charge or sentencing in Australia.

There is nothing expressly analogous in Australia to the 'anti-piling on' policy in the United States.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common, per se. Ordinarily, any negotiations regarding settlement in Australia will take into account the settlements or negotiations for them in other jurisdictions.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Given the co-operation mechanisms available to Australian regulators (such as mutual assistance agreements and the International Organization of Securities Commissions' Multilateral Memorandum of Understanding), it is possible to conduct concurrent investigations in multiple jurisdictions regarding the same factual matters. It is usual for one or more Australian investigatory bodies to coordinate domestically and with international investigatory bodies. A coordinated effort will usually result in one regulator taking the lead in an investigation and other jurisdictions supporting its efforts to round out the information gathering. This is not always the case, however, and therefore strategic calls as to regulatory co-operation may need to be made quickly in a variety of jurisdictions.

© Law Business Research 2021

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The administration and implementation of Australia's sanctions laws is carried out at federal level by the Department of Foreign Affairs and Trade (DFAT). From 1 January 2020, the Australian Sanctions Office, part of DFAT, became the national sanctions regulator. There is a dedicated sanctions portal, Pax, which encourages Australians to ask about sanctions, request assessments or apply for permits. Sanctions are implemented in accordance with (1) the United Nations Security Council (UNSC) regime and (2) an autonomous, Australia-specific sanctions regime. DFAT has the power to issue a sanctions permit, should it be suitable, which will allow an importer or exporter to undertake activity that would otherwise contravene a sanction imposed in Australia. A full list of Australia's sanctions regimes is publicly available and it is expected that individuals and companies doing business in Australia should make their own enquiries to ensure compliance.

Sanctions against both individuals and entities are constantly being updated. In April 2019, Australia imposed sanctions on the direct or indirect supply, sale or transfer to the Central African Republic of arms or related materials without the issuance of a sanctions permit. In March 2019, Australia issued autonomous 'financial sanctions and travel bans on seven Russian individuals for their role in the interception and seizure of Ukrainian naval vessels'. In February 2020, a number of individuals were included in financial sanctions and travel bans as 'elected' members of the Republic of Crimea and Sevastopol.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Australia is obliged to closely follow the UNSC in relation to enforcement of sanctions. Contraventions are enforceable against Australian individuals and companies, and certain sanctions will have effect irrespective of whether the activities have taken place in Australia or overseas. The Australian government has successfully prosecuted a number of companies for sanctions violations. A small number of Australian individuals have also been charged, including one who was convicted of breaching sanctions laws in 2021 in respect of activities in North Korea. He was sentenced to three and a half years' imprisonment.

In recent times, there has been discussion as to whether sanctions enforcement should also more readily incorporate the Australian Transaction Reports and Analysis Centre, which regulates cross-border monetary transactions, including money laundering and the financing of terrorism.

© Law Business Research 2021

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

DFAT may consult other government agencies, other countries or the Sanctions Committee of the UNSC on a range of issues, including in consideration of whether to agree to a sanctions permit.

Australia is also a member of the Financial Action Task Force (FATF), which is the global money laundering and terrorist financing regulatory body setting international standards with the aim of preventing global money laundering and terrorism financing. FATF recommendations have included the need for implementation of targeted financial sanctions as critical to combat these illicit activities.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Australia currently does not have blocking legislation in relation to sanctions measures taken by third countries.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

There are a number of ways in which misconduct can be brought to the attention of a company, including the following:

- The Australian Securities and Investments Commission (ASIC) conducts a preliminary investigation into every allegation of misconduct to assess whether further action is required. ASIC may be made aware of suspected contraventions by shareholders, media reports or whistleblowers.
- Whistleblower legislation requires that certain companies have whistleblower policies in place that include avenues for employees to report suspected misconduct. These reports may trigger internal investigations or investigations by ASIC. In 2019, following enhancements to whistleblower legislation and protection, ASIC established the Office of the Whistleblower. Further, companies will often have policies and practices in place, such as audit procedures or due diligence requirements, which may bring to light misconduct. Australian companies, often with operations, parent or subsidiary companies overseas, generally work towards international best practice.
- The Australian Transaction Reports and Analysis Centre monitors international transactions and transactions of A$10,000 (or more) and will investigate any suspicious transactions under anti-money laundering and counter-terrorism legislation. It

© Law Business Research 2021

is mandatory to report suspicious transactions (such as money laundering, terrorism financing, operating under a false identity, tax evasion or the proceeds of crime) within 24 hours if the transaction relates to terrorism, or otherwise three business days.

- The Australian Securities Exchange (ASX) monitors share trading in publicly listed companies and can inquire into suspicious activities, including spikes in trading volume or share price. The ASX can refer suspected contraventions (such as insider trading) to ASIC for further investigation.
- Since 2018, the Financial Services Royal Commission has been a significant source of reporting of misconduct in the Australian financial services industry. Regulatory activity has increased as a result, including the institution of court proceedings and a number of high-profile settlements with regulators such as ASIC.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The Privacy Act 1988 (Cth) (the Privacy Act) regulates the handling of personal information and the Australian Privacy Principles (APPs) provide guidelines for dealing with such information. The Notifiable Data Breaches scheme, established through the Privacy Act, obliges entities to notify individuals whose personal information is the subject of a data breach and the Office of the Australian Information Commissioner (OAIC), when it is likely the breach will result in serious harm.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The data protection regime is enforced through the OAIC. The Privacy Act confers powers on the Commissioner to facilitate compliance with best practice. The OAIC's preferred regulatory approach is to facilitate compliance and prevent breaches, although it also has investigative and enforcement powers. In December 2020, the OAIC made a submission as part of the Privacy Act Review being undertaken by the Attorney General's Department, advocating for greater enforcement powers, organisational accountability and greater interoperability. A discussion paper, including possible reforms of the Privacy Act, was released in 2021, seeking feedback by early 2022.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The APPs regulate how personal information is collected and used. If an entity investigates the actions of an employee, it must be careful that any personal data is collected in accordance with these principles. A heightened level of protection attaches to sensitive information, such as a person's religious beliefs, sexual orientation or health information. Entities must comply with their legal obligations, particularly those that require an employee to be notified that personal data has been collected. It is also important to consider any implications of cross-border transfer of personal information and the interplay with legal obligations in other jurisdictions, which at times can be stricter than those in Australia.

© Law Business Research 2021

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Employers are bound by contractual arrangements with employees, which often specify the rights an employer has over communications made during the course of employment. Interception of employment-based communications can be triggered by an internal investigation or well-founded suspicion of a contravention of company policy or legal obligations. Interception of personal, non-work-associated communications is governed by strictly applied privacy and telecommunications legislation and is likely to be illegal if beyond the scope of the employment arrangement and without consent.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Generally, the Australian Federal Police (AFP) executes search warrants on behalf of Commonwealth agencies. If an investigation is being conducted by another regulatory body, AFP officers may attend with officers of that regulatory body. Warrants contain information as to the restrictions on entry time, dates and the evidence that can be gathered during the execution of the search warrant, which may include hard copies of documents as well as stored communications (such as computer hard drives or mobile phones). Defendants are entitled to observe the search being undertaken, to have legal representatives present and to request an itemised list of the property seized, and have a right to challenge the warrant's validity.

Legislation introduced in 2020, known as the Stronger Regulators Act, has strengthened the search warrant powers of the Australian Securities and Investments Commission (ASIC) by allowing the Commission to seize evidential materials, instead of the more restrictive 'books' under previous legislation, if the evidential materials are seized in connection with an indictable offence. Further, once materials have been seized, they can now be used for civil penalty proceedings, not just criminal proceedings.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Defendants may claim legal professional privilege (LPP) over materials seized during a legitimate search. Practically, this may mean the materials are sealed and delivered to the relevant court registry or regulator to await resolution of any disputed privilege claim by litigation or negotiation. The mere seizure of material without it being read does not constitute a waiver of privilege.

For disclosures to ASIC, companies can agree to enter into a voluntary confidential legal professional privilege disclosure agreement, which would provide ASIC with privileged documentation, without waiving privilege over those documents. This may be particularly useful for companies seeking a co-operative approach with the regulator but

© Law Business Research 2021

wanting to reduce the risk of losing the rights available to them. The efficacy of ASIC's voluntary disclosure agreement has not been tested in the courts.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

During an investigation by a regulator, an individual can usually be compelled to give evidence in an examination. The individual cannot refuse to answer questions on the basis that those answers may tend to incriminate him or her. However, the individual can claim privilege against self-incrimination, meaning that the investigatory body cannot use the evidence gathered as an admission by the individual. Some regulatory bodies can derivatively use the information gathered during these types of examinations.

In a litigation context, an accused person has a right to claim privilege against self-incrimination or self-exposure to penalty, which means that they cannot be required to give evidence during proceedings against them. An exception to this is if the accused, or a witness, is asked to give evidence on a topic that is not the subject of the trial but would tend to incriminate them in other proceedings. The witness can seek a certificate, under section 128 of the Evidence Act 1995 (Cth) or the state-based equivalent, which, in essence, compels an answer but protects the witness from self-incrimination. A witness may object to giving evidence in proceedings if the response would tend to prove that the witness had committed an offence under Australian or foreign laws, or make him or her liable to a civil penalty.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Whistleblower protections are captured under the Corporations Act 2001 (Cth) (the Corporations Act) and apply to both current and former employees within a defined list of roles. The legislation outlines the reporting lines and the role of a corporation in affording protections to whistleblowers. It is a strict liability offence for certain companies not to have a company policy relating to whistleblowing.

There is no financial incentive programme in Australia for whistleblowers.

Corporate whistleblowers who provide information to the Australian Securities and Investments Commission (ASIC) about contraventions of the Corporations Act are granted three main legal protections, which are that:

- their identity and the information given cannot be disclosed unless authorised by law;
- they are protected against civil or criminal liability for making the disclosure (e.g., for defamation); and
- they are protected against being victimised for making their disclosure.

© Law Business Research 2021

ASIC has provided industry guidance, under Regulatory Guide 270, to assist companies in understanding the requirements for a whistleblower policy and providing guidance on good practice for implementing and maintaining their policies.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Under the Fair Work Act 2009 (Cth), certain employees are protected against unfair dismissal. In the event of an internal investigation, certain omissions by the employer may violate the right against unfair dismissal, including failing to provide the employee with a support person. The employee has a right to be given information relating to the allegations against him or her and adequate time to respond.

Under the Corporations Act, officers and directors are subject to significantly higher standards of conduct. Contravention of these duties may attract significant penalties, disqualification or imprisonment.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

If an employee has engaged in misconduct, his or her rights will depend on the precise nature of the misconduct. For example, an internal finding of serious misconduct may constitute valid grounds for dismissal. However, a finding of serious misconduct by law enforcement may constitute an offence, and the employee's rights would depend on the associated laws.

There are no express requirements for employers to impose disciplinary or other steps if an employee is suspected of misconduct.

If 'serious misconduct' is established, the employee's contract of employment may be immediately terminated. The Fair Work Regulations 2009 (Cth) define 'serious misconduct' as including wilful or deliberate behaviour that causes serious or imminent risk to the health or safety of employees or reputation to business; examples include theft, fraud, assault, being intoxicated at work, or refusing to carry out lawful and reasonable instructions.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Mere refusal to participate in an internal investigation is unlikely to constitute valid grounds for dismissal. However, an employee may open himself or herself up to grounds for dismissal if the refusal is deemed to be a breach of a reasonable direction given by the employer.

© Law Business Research 2021

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common to set out the scope of an investigation before it commences, although this is not mandatory. Consideration should be given to any regulatory compliance obligations, including reporting obligations. It is common for a board of directors to refer an internal investigation to an external adviser, such as a law firm, particularly if the board has concerns about litigation and risk management and would like the investigation to be covered by legal professional privilege.

Terms of reference, if prepared, should outline the key allegations or concerns, define the sources of information that it is proposed should be gathered during the investigation, and identify who will report on the findings or recommendations of the investigation and the recipient of the report.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

When a company becomes aware of potential issues, an investigation should be undertaken to identify the nature and extent of any misconduct. Care should be taken in setting up the investigation, including to ensure that communications are confidential and privileged to the extent possible.

A company may be obliged to report to regulators in relation to certain breaches, or may elect to self-report or seek immunity. Legal advice should be sought prior to making such decisions as the consequences may be serious. Guidelines are available for various breaches, such as foreign bribery and breaches of licences.

A company should work towards containing the breaches and, as far as possible, secure complete cessation of the offending behaviour. Evidence of the suspected breaches should not be destroyed and document preservation notices should be issued in appropriate circumstances. Any dismissal or discipline of individuals suspected to have participated in the misconduct should be carefully managed and based on legal advice.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Compulsory document production notices must be strictly complied with as it is a criminal offence not to do so without a reasonable excuse. The notice may be addressed to an individual or the 'appropriate officer' within the company. The named individual does not have to coordinate the response but they should be kept informed as they may be held personally liable for any non-compliance. It is usually advisable to seek legal advice regarding notices and often advisers can become a point of contact with the regulatory agency. For smaller organisations, such an approach may alleviate the need for persons

© Law Business Research 2021

of interest in the investigation to liaise directly with investigators and avoid unwittingly waiving fundamental rights that could attach to that status.

It is necessary to make 'reasonable endeavours' to respond to a notice. A structured approach to the collation and production of materials should be taken, including where data will be sourced, relevant individuals or custodians of data, document preservation, and how the documents will be collated and stored to preserve original documents and metadata. A subpoena, requiring production of documents to a court, must also be complied with. The same considerations should be made by a company issued with a subpoena to produce.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

If the internal investigation is confidential, there is no requirement for a company to disclose the existence of the investigation publicly. Disclosure may be desirable or required if it is not possible for the conduct to be contained or if media or market speculation needs to be addressed. If the company is being investigated by regulators, disclosure will often depend on the preferred approach of that regulator. It is usual for regulators to ask that disclosure of the fact of their investigation not be made public unless mutually agreed. However, continuous disclosure obligations for listed companies must also be considered to the extent that they apply.

Private companies have no legislative obligation to disclose the existence of an internal investigation or contact from law enforcement.

37 How are internal investigations viewed by local enforcement bodies in your country?

An efficiently run internal investigation may be welcomed by the regulator, particularly if it leads to self-reporting. In some circumstances, a regulator may ask the corporate entity to undertake the first stage of the investigation. If an internal investigation is running concurrently with a regulator's investigation, co-operation in expediting the process and ultimate outcome is encouraged.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Communications made for the dominant purpose of giving or receiving legal advice, or regarding the provision of professional legal services for existing or contemplated litigation, can be subject to a legitimate claim for legal professional privilege (LPP). If there is more than one purpose relating to an investigation, it is unlikely that the communication will be privileged.

© Law Business Research 2021

Lawyers' notes regarding internal investigations are usually protected by LPP. To protect the privilege, all communications should be marked as confidential and privileged and should not be distributed outside the lawyer–client communication lines unless necessary.

A 2021 Federal Court decision in a cartel matter saw privilege over entire documents lost when the company, which was under an obligation to co-operate with regulators in return for being granted immunity, provided the regulators with extracts of the privileged documents. The court ordered that the documents could not be properly understood unless read in full and therefore privilege had been lost in respect of the entire document. The case highlights the complexities faced by companies seeking protection from prosecution, while attempting to maintain the rights ordinarily afforded to them.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

LPP is held by the client (company or individual), not the legal adviser. Employees of the company may have grounds to assert common interest privilege or joint privilege, if the employee reasonably believed the lawyer was giving them legal advice and his or her interests were not adverse to the company. If a company seeks to maintain control over the privileged information, lawyers will ordinarily be instructed to communicate that distinction, adopting a US-style *Upjohn* or corporate *Miranda* warning.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes. The dominant purpose test applies, irrespective of whether the lawyer is internal or external to the company. Best practice is for in-house counsel to hold a current practising certificate and be independent. Privilege claims of advice from in-house counsel generally will be scrutinised, particularly if another non-legal position is held within the company, or if counsel is accustomed to providing commercial advice (which will not be privileged).

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Yes. Australian clients can claim the privilege if the communications are with a qualified lawyer admitted to practise in the foreign country and the communications satisfy the dominant purpose test.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

It is normal for companies and individuals to maintain claims of LPP. Waivers are generally restricted to circumstances in which the entity is essentially opening its doors on a no-restrictions basis, has been done on a limited basis subject to agreement, such as in

© Law Business Research 2021

co-operation with a regulator or if a party is obliged to waive privilege in furtherance of an agreement for immunity. It may be considered that not claiming LPP signals an increased level of co-operation with the investigating authority. A court, tribunal or commissioner to a royal commission may compel an entity to produce documents if it has been determined that the claims for privilege cannot be maintained. Regulators are increasingly challenging claims for LPP, including taking some matters to court to dispute claims by companies withholding production of documents on the basis of LPP.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. For instance, a party responding to a compulsory notice to produce documents to the Australian Securities and Investments Commission (ASIC) may enter into a voluntary confidential LPP disclosure agreement, which allows production of the documents to ASIC, while arguably protecting them from disclosure to third parties. ASIC will undertake to treat the information as confidential and will defer to the privilege holder if ASIC is compelled to produce the documents. These agreements have not been tested by the courts as to whether they will withstand a challenge.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Possibly. Relevant considerations will include the context in which the waiver was made (under compulsion or voluntarily), the use of the information subsequent to the waiver and whether, in Australia, privilege would still properly apply to the information.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist. The interest of the parties claiming the privilege must be the same, or almost the same (such that the parties could use the same lawyer), and it will not be available if they are potentially adverse. There is no requirement for a formal agreement between parties to establish this privilege, nor to identify an intention to claim the privilege at the time of communication, although it is advisable to do so to establish the extent of the common interest.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

It is not uncommon for lawyers to brief third-party experts to assist on matters relevant to the giving of legal advice. Communications with the third party will usually be covered by LPP if they fall within the dominant purpose test.

If a party serves a report or advice prepared by a third party during litigation, all materials (including briefing materials) used by the third party in informing an opinion generally become discoverable. There are limited circumstances in which a party can resist production of communications underpinning a report.

© Law Business Research 2021

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Organisations are permitted to conduct fact-finding interviews during an internal investigation. Consideration should be given to ensuring that the individual is afforded the appropriate amount of time to prepare and respond to questions. Whistleblowers, who may be among the first interviewed, are afforded additional legislative protections that must be adhered to. Immunity applicants are required to keep confidential any fact that commentators have indicated could be a complication in internal investigations.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Legal professional privilege can be claimed over witness interviews and reports prepared by legal advisers for the dominant purpose of giving or receiving legal advice or in the preparation of legal proceedings.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Corporate *Miranda* or *Upjohn* warnings are not required to be given, although they are common in cross-border investigations. It is prudent to outline the scope of a lawyer's engagement at the time of the interview, to avoid any misconception as to whether the parties intend privilege to apply. The same approach applies to both current employees and third parties, although there is less scope for privilege to apply to third parties.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There are no set requirements for internal interviews in Australia and often the style of interview will depend on the seriousness of the allegations being investigated. Notes of interviews should be kept confidential and a record of any materials discussed during an interview should be retained for future reference. Generally, a witness will be asked for an independent recollection of events before being presented with any documents. Documents put to a witness are usually restricted to those about which the witness has first-hand knowledge. If the allegations are serious and directed to the interviewee, then it is not unusual to provide the interviewee with the option of having their own legal representation at the interview, though an interviewee may not necessarily have an enforceable right to have their own legal representation.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

It is mandatory under anti-money laundering and counter-terrorism financing legislation to report suspicious financial transactions to Australian Transaction Reports and Analysis Centre. The company must have formed a suspicion that the dealings may be related to an offence (such as money laundering, terrorism financing or operating under a false identity, tax evasion or proceeds of crime) and must report within 24 hours if it relates to terrorism, or otherwise three business days.

Australian financial services licensees must report any significant breaches, or anticipated breaches, of obligations under the Corporations Act 2001 (Cth).

State legislation may also apply. In New South Wales, for instance, it is an offence to conceal knowledge or belief of a serious indictable offence having been committed. This provision is unique to New South Wales.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

If an internal investigation has led to findings of misconduct, a decision will need to be made whether to self-report. Self-reporting may be advisable if the findings are likely to affect the company's ability to conduct its business or trading of the company's shares.

Disclosure to regulators outside Australia may depend on whether the conduct has occurred outside the jurisdiction and the reporting obligations in those other jurisdictions.

Companies often make a decision to self-report to regulators, either when dealing with multiple jurisdictions within the country, or internationally if they expect public attention arising from the investigation. This is often considered to be 'controlling the message' to both the public and regulators.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

In self-reporting, the company should be prepared to co-operate honestly and completely with authorities and assist regulators' investigations, which may go beyond internal investigation. This may involve providing to authorities any information gathered during the internal investigation at the time of self-reporting. There is an added benefit in creating a clear line of reporting between the company and the regulator.

The company should be prepared to plead guilty to any offence identified and may be required to assist in the prosecution of related parties. Public disclosure will need to be considered for listed companies, consistent with disclosure obligations.

In certain circumstances, immunity for being first-in-time can be sought when reporting to the Australian Competition and Consumer Commission or the Australian Securities and Investments Commission.

© Law Business Research 2021

Legislation allowing deferred prosecution agreements is proceeding through the Parliament of Australia. It has been the subject of extensive consultation and the timing for its implementation is not yet known. Once passed, it is anticipated that this legislation will provide benefits to corporates who self-report relevant offences.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Companies take seriously their obligation to comply with compulsory production requests from regulators. It is possible to enter into a dialogue with a regulator in relation to a notice or subpoena, particularly if there are concerns about scope or time for production. This is done by speaking or writing to a representative of the regulator in the first instance.

In recent years, Australian regulators have indicated a greater willingness to engage with companies to address concerns or to encourage self-reporting of misconduct prior to the issuing of charges. If in the course of preparing a response to the compulsory production request, broader issues are identified by a company, the current environment encourages discussion with regulators. Post-charge negotiation in criminal proceedings is governed by the relevant prosecution policy.

55 Are ongoing authority investigations subject to challenge before the courts?

A company may challenge an investigation in particular circumstances, for example if the investigation is an abuse of process or harassment.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Consistency is key when a company is facing allegations of wrongdoing regarding the same facts in multiple jurisdictions. A company should ensure responses are coordinated and that production of documents or information is strictly responsive to the notice or subpoena. There is no requirement to go beyond the strict terms of the notice or subpoena and doing so may amount to voluntary disclosure and not be afforded protections (such as confidentiality and privilege) that would otherwise be available.

© Law Business Research 2021

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Materials must be produced if they are in the possession, custody or control of a company in Australia (irrespective of the location where they are held). It may be possible to resist production of materials outside Australia if to do so would be oppressive or if their production was contrary to the law of the jurisdiction where the documents are located.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Australian regulators routinely share information or investigative material and make use of mutual recognition agreements with regulators from other jurisdictions, such as the International Organisation of Securities Commissions. Less formal arrangements exist between some regulators, such as the Australian Federal Police's arrangements with other police agencies globally. Mutual assistance requests are a formal mechanism by which authorities can obtain information from overseas regulators for use in criminal proceedings.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Information produced under compulsion can only be used for the purpose for which it was obtained. Materials can be shared between regulators, subject to satisfying legislative requirements, and can be disclosed to third parties during an investigation if it is deemed necessary and legislative requirements are satisfied.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Refusing to produce a document that is required under a notice will be a breach and may give rise to legal action by the regulator. Open dialogue with the regulator is encouraged at an early stage to attempt to negotiate an amendment to the notice to exclude production of documents that give rise to a breach of laws in another jurisdiction. Otherwise, the company should look at avenues to challenge the notice.

© Law Business Research 2021

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Australian data privacy laws prevent the disclosure of certain personal and sensitive information. The Australian Privacy Principles (APPs) apply to government agencies, private sector and not-for-profit organisations (those with an annual turnover of more than A$3 million), private health providers and small businesses.

Disclosure is permitted if compelled (such as by a document production notice or subpoena) or reasonably necessary for one or more enforcement-related activities by an enforcement body. In defending allegations of misconduct, data may also be transferred for the purposes of, or in connection with, legal proceedings (including prospective legal proceedings) or for the purposes of establishing, exercising or defending legal rights. However, restrictions on the cross-border transfer of data may remain.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

It is common for companies to request that a regulator issue a notice to compel the production of materials to preserve claims of confidentiality and privilege. Such a claim may be waived by voluntary production. Regulators can be compelled to produce documents to third parties by court order, but may segregate documents that are subject to claims of privilege (including legal professional privilege and public interest immunity) and confidentiality, and leave it to the court to rule on such claims. However, in limited circumstances a company may identify a reputational risk in the use of compulsory production notices and a co-operative approach may be preferred. A company should weigh up the merits and ramifications of each approach.

The APPs should be considered when voluntarily producing materials to authorities, as this will not fall under the exemption of compelled production.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies can face significant financial penalties for criminal misconduct, calculated at the greater of 45,000 penalty units (currently A$9.45 million), three times the benefit derived or detriment avoided, or 10 per cent of annual turnover. Civil penalties are also available against a company and vary greatly according to the relevant provisions. The maximum civil penalty available against a company is the greater of 50,000 penalty units (A$11.1 million), three times the benefit obtained or detriment avoided, or 10 per cent of annual turnover, capped at 2.5 million penalty units (A$555 million).

Penalties against an individual will vary depending on the offence. Criminal wrongdoing may result in imprisonment or financial penalties, or both. Civil penalty proceedings can result in fines, compensation orders and disqualification from managing

© Law Business Research 2021

corporations. In certain circumstances, administrative action to seek banning orders may also be commenced.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The Commonwealth, state and territory governments do not automatically suspend or disbar a company for any conduct, although they do have discretion to preclude a company from public procurement contracts.

65 What do the authorities in your country take into account when fixing penalties?

Courts will consider a range of factors, including the seriousness of the offence, the number of contraventions and the period during which they occurred, the need for general deterrence, remorse, retribution, co-operation and any relevant personal circumstances. In light of applicable high court authority, a prosecutor cannot recommend to a court a preferred criminal sanction, such as a prison sentence for an individual. In civil penalty proceedings, a proposed penalty can be agreed between the parties in settlement discussions and this can be jointly presented to the court. The court is not required to accept the negotiated penalty figure but can (and often will) take the negotiated outcome into consideration when ordering penalties.

In recent years, there has been a significant increase in penalty amounts set by legislators and applied in the courts for corporate misconduct. This is mostly attributable to the significant increase in penalty limits available to the Australian Securities and Investments Commission since the passing of revised legislation in February 2019, when the regulator publicly announced its intention to pursue harsher civil penalties and criminal sanctions.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Deferred prosecution agreements (DPAs) are not currently available but draft legislation is before Parliament, which may lead to them being introduced. Based on the current proposed legislation, DPAs will allow companies to negotiate terms of settlement for allegations of serious corporate crime, such as foreign bribery, which include the setting of a penalty for contravention, but will require approval by an approving officer (a former judicial officer) before they can be finalised. Not all corporate crimes are covered in the proposed legislation and DPAs will not be available to individuals.

DPAs under the proposed legislation are similar to non-prosecution agreements under US law.

Another mechanism in which a company may reach agreement with authorities to avoid prosecution in return for co-operation is by seeking an indemnity, more formally referred to as an undertaking, under the Director of Public Prosecutions Act 1983 (Cth). The circumstances in which an indemnity may be granted are generally governed by

© Law Business Research 2021

the Prosecution Policy of the Commonwealth. In the context of cartel prosecutions, applications are governed by the Australian Competition and Consumer Commission's Immunity and Cooperation Policy for Cartel Conduct. In February 2021, the Australian Securities and Investments Commission (ASIC) introduced an immunity policy, available to individuals seeking protection for contraventions of certain market misconduct offences under the Corporations Act 2001 (Cth).

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no certainty regarding implementation of DPAs in Australia at present; however, the Bill currently proceeding through Parliament proposes that a DPA be published in full, except in exceptional circumstances, such as when the publication would prejudice court proceedings. This approach is consistent with that currently adopted when a company has pleaded guilty, or been granted an indemnity from prosecution, but proceedings against connected individuals or corporate entities are continuing (such as in the case of cartel proceedings).

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Considerations relevant to settlement include an assessment of the facts and allegations made against the company, the strength of the evidence, the terms on which the regulator is willing to settle (where they can be agreed) and the potential consequences of any settlement (including on business operations, investigations in other jurisdictions and the risk of collateral civil litigation). These considerations generally apply only in the context of civil penalty proceedings, with criminal proceedings presently unable to be 'settled' in the traditional sense.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The proposed DPA process suggests the use of an independent monitor, paid for by the company, to assess compliance with the terms of the DPA. The reason for this is, in part, that the body responsible for entering into DPAs with companies, the Commonwealth Director of Public Prosecutions, does not have a monitoring function. External corporate compliance monitors have also often had a role in enforceable undertakings with ASIC. The Australian Prudential Regulatory Authority and the Australian Transaction Reports and Analysis Centre also use independent reviewers in these tools.

© Law Business Research 2021

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private actions are permitted to run in parallel with criminal or regulatory proceedings, provided they do not prejudice the accused's right to a fair trial, or the right to maintain privilege against self-incrimination or exposure to penalty, and do not interfere with the criminal proceedings. It is possible for private or civil actions to be stayed pending the outcome of criminal proceedings.

Private plaintiffs are entitled to apply to regulators to access files through various mechanisms, including freedom of information requests and subpoenas. In addition, ASIC has the power to provide information to private litigants in certain circumstances. The disclosure of information by regulatory bodies is subject to overriding considerations of public interest, the risk of prejudice to an ongoing investigation or proceeding, and statutory restrictions.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Criminal investigations are generally confidential. An accused has the right to a fair trial and a presumption of innocence. Investigatory bodies, such as the Australian Federal Police and the Australian Securities and Investments Commission, have media policies that restrict the publication of information that may prejudice an ongoing investigation or affect an accused's right to a fair trial, particularly in tainting the jury pool.

Criminal court proceedings are a matter of public record. There are limited situations in which a corporation or individual can restrict access to, or publication of, the court proceedings once they are formally commenced. Although the media are entitled to report on public hearings, they are required to follow orders from the judge concerning non-publication of certain information.

Jury deliberations are confidential. It is an offence to publish anything regarding the identity of a juror or the discussions that take place in the jury room.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for public relations firms to be hired, particularly in high-profile matters. Lawyers will generally work with a public relations firm hired in these circumstances to provide strategic advice, to ensure accuracy of reporting and in making any public statements during an investigation or proceeding.

73 How is publicity managed when there are ongoing related proceedings?

Corporations need to carefully manage the release of information regarding ongoing proceedings to avoid being in contempt of, or prejudicing, the proceedings, especially any criminal proceedings before a jury, and to meet any relevant continuous disclosure

© Law Business Research 2021

obligations. Regulators will announce the commencement of proceedings and may provide procedural updates but generally will not comment on substantive matters for the duration of the proceeding.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

If the settlement is likely to have a material effect on the price or value of the company's securities and does not fall within an exception (such as the information being confidential), it is required to be disclosed to the market by a public company. Confidentiality alone is not grounds for non-disclosure of the fact of settlement. It is often the case that parties agree the terms of disclosure of a settlement as part of the settlement negotiations.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

The absence of an Australian standard approach to ESG reporting often increases the cost and complexity of compliance for investors, with requirements found in a variety of state and federal legislation. For instance, the Corporations Act 2001 (Cth) (the Corporations Act) regulates company governance and the duties and obligations of directors and officers, and the rights and interests of aboriginal and Torres Strait islanders is primary governed by the Native Title Act 1993 (Cth) and requires corporations to comply with native title claims.

Workplace governance standards such as workers' rights are covered in a number of state and federal statutes. Whistleblower protections are incorporated in the Corporations Act. Legislation such as the Fair Work Act 2009 (Cth), the Workplace Gender Equality Act 2012 (Cth), the Modern Slavery Act 2018 (Cth) (the Modern Slavery Act) and various state and territory equivalent legislation cover rights and obligations for workers. Unlike other jurisdictions, the reporting criteria in Australia is mandatory under the Modern Slavery Act.

Environmental laws are also covered on both a federal and state or territory level, with the primary legislation being the Environment Protection and Biodiversity Conservation Act 1999 (Cth). Other state-based legislation covers a range of matters, such as waste management and contamination. Major facilities are legislatively required to meet reporting obligations under the National Greenhouse and Energy Reporting Act 2007.

A number of voluntary and statutory measurement, reporting and disclosure frameworks are used in Australia with respect to ESG. In addition to international standards such as the UN Principles of Responsible Investment, there are various voluntary standards and best practices that are commonly followed with respect to integrating ESG factors into investment decisions, including those released by the Responsible Investment Association Australasia, the Australian Council of Superannuation Investors (ACSI) and the Investor Group on Climate Change.

© Law Business Research 2021

When it comes to ESG reporting and disclosure frameworks in Australia, the obligation regime (e.g., mandatory versus 'comply or explain') for companies often depends on whether or not they are listed. By way of example, Australian Securities Exchange (ASX) Listing Rule 4.10.3 requires a listed entity to include certain information in its annual report, including a corporate governance statement that meets the requirements of that rule, or the URL of the page on its website where a corporate governance statement that meets the requirements of that rule is located. A corporate governance statement must disclose the extent to which that listed entity has followed the recommendations set by the ASX Corporate Governance Council during the relevant reporting period or the reasons for not following the recommendation and what (if any) alternative governance practices it adopted in lieu of the recommendation during that period.

As of 1 January 2020, the ASX Corporate Governance Principles and Recommendations issued by the ASX Corporate Governance Council recommend that listed entities benchmark certain corporate governance practices that are the 'reasonable expectation of most investors', including topics such as board diversity and sustainability disclosures. In particular, Recommendation 1.5 ('A listed entity should have and disclose a diversity policy') and Recommendation 7.4 ('A listed entity should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks') should be noted.

The ESG Reporting Guide for Australian Companies released by ACSI and the Financial Services Council is commonly adopted voluntarily by both listed and unlisted companies to assist with their understanding, pricing, analysis and management of ESG investment risks. It is designed to complement the reporting requirements of other best practice guides, such as the ASX Corporate Governance Principles and Recommendations.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Australian regulators have shown an increased appetite to address failings in the disclosure and management of non-financial risks, with a growing number of these being ESG-related.

In 2019, the Australian Securities and Investments Commission (ASIC) updated a raft of regulatory guidance and information notes to specifically refer to climate change considerations in corporate governance. ASIC recognises the Taskforce for Climate-related Financial Disclosures, established by the Financial Stability Board, and recommends that listed companies adopt the framework and guidance provided by the Taskforce. ASIC conducts surveillance, including examinations of large listed companies, and has indicated that adopting the Taskforce's reporting materially improves the standards of climate-related governance and disclosure in the market. ASIC is considering enforcement action in circumstances of serious disclosure failures.

Similarly, the Australian Prudential Regulatory Authority (APRA) encourages the adoption of the Taskforce's frameworks, as noted in its letter to APRA-regulated entities in 2020. APRA proposes to produce a practice guide to assist its members.

The ASX makes mention of the Taskforce's frameworks, encouraging entities to consider whether they have a material exposure to climate change risk, in its 2019 Corporate Governance Principles and Recommendations.

© Law Business Research 2021

The Organisation for Economic Co-operation and Development (OECD) has commented that Australia is one of the most resource-intensive and carbon-intensive OECD countries and that the state of its biodiversity is poor and worsening. Significant criticism and pressure has been placed on the Australian government to address greenhouse emissions and to combat climate change issues.

Climate change proposals from shareholders at companies' annual general meetings (AGMs) are driving greater levels of ESG-linked reporting among boards and directors. For example, shareholders can apply pressure by using a special resolution to amend a company's constitution regarding the way in which a power vested in the directors has been, or should be, exercised. Shareholders can then propose resolutions (contingent on the passing of the special resolution) regarding a specific matter – for example, the reporting of climate change management. Details of these 'proposed contingent resolutions' are later released on the company's ASX AGM results announcement. It is anticipated that shareholder pressure through means such as this will drive regulatory or legislative change in the future.

Directors' exposure to personal liability for climate change inaction is a live issue that has received endorsement by ASIC and the legal profession. Climate risk and disclosure have become a shared focus of Australian financial regulators and investor groups, engaging questions about directors' personal liability for associated corporate inaction. Following the 'Climate Change and Directors' Duties Memorandum of Opinion' (7 October 2016) (the Opinion) and the 'Climate Change and Directors' Duties Supplementary Memorandum of Opinion' (26 March 2019) by The Centre for Policy Development (the Supplementary Opinion), there is an emerging view that a director's duty to act with reasonable care and diligence under section 180 of the Corporations Act positively mandates the active identification, proper disclosure and appropriate response to foreseeable climate change risks. In predicting the 'exponential' increase of individual directors' personal exposure to climate change litigation, the Supplementary Opinion rejects any scenario going forward whereby 'climate change will not intersect with the interests of [their] firms', citing relevant advances in 'event attribution science' capable of identifying the link between climate change and individual extreme weather events.

Companies should also consider the derivative risks for directors arising from the ASX Guidelines on ESG-linked reporting.

From a practical standpoint, the issues of directors' personal liability for climate change have a direct effect on business operations; as such, maintaining strong effective corporate governance has received endorsement by both the ASIC Commissioners and former Australian High Court Justice Kenneth Hayne SC.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Like many other jurisdictions, ESG issues are an important topic on a range of fronts. Australia has seen an increase in investigations relating to ESG across a full spectrum of issues.

An inquiry into sexual harassment against women in the FIFO (fly-in, fly-out) mining industry brings to the forefront discussions regarding the health and safety of workers in Western Australia. Most major mining companies with operations in Australia have

© Law Business Research 2021

indicated overwhelming support for the inquiry and a promise to engage in the issues arising from the evidence.

Climate-related litigation, both privately led and regulator-led, has already been an area of focus in Australia, with long history and a number of high-profile cases in the courts. The Australian Competition and Consumer Commission has historically commenced a number of cases against car companies for claims that their products were environmentally friendly (*Goodyear Tyres*, 2008) or advertised as green, with carbon emissions neutral across the range (GM Holden's claims regarding its Saab vehicles, 2008). A class action against the Commonwealth Bank of Australia in 2017 was ultimately withdrawn by shareholders, but nevertheless resulted in the bank reporting on the risk of climate change and pledging to undertake climate change scenario analysis to estimate the risks to its business. A settlement in *McVeigh v. Retail Employees Superannuation Trust* (REST being one of Australia's largest superannuation funds) resulted in a commitment by REST to new disclosure protocols and climate change-related initiatives.

In 2020, the Australian government was sued by a Melbourne law student for failing in its duty to disclose the effects of climate change on the value of government bonds. This case is ongoing.

ASIC announced in July 2021 that it is reviewing offerings by managed funds and superannuation funds providing investment products focused on ESG and the concern regarding the potential for 'greenwashing' of financial products.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The corporate and legal community eagerly await any developments in draft legislation that will introduce deferred prosecution agreements and amendments to the anti-bribery and corruption legislation (a topic that has been discussed since 2017). The current draft legislation has been before Parliament since 2019. There is currently no indication of when further movement on this legislation will occur.

Regulators such as the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission have communicated their increased focus on consumer protection in areas such as cybersecurity, which has become an increasing risk to consumers during lockdown periods arising from covid-19 outbreaks. The effects on corporations will be seen in the security measures put in place to protect their customers.

© Law Business Research 2021

7

Brazil

Heloísa Barroso Uelze, Felipe Noronha Ferenzini and João Augusto Gameiro[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Operation Car Wash is the largest corruption and money-laundering investigation in Brazil and related developments continue to occur.

However, owing to the covid-19 pandemic, the spotlight turned to several police investigations involving state and municipal governments in relation to alleged undue public expenditure on health-related measures. Several types of alleged irregularities have been claimed in the construction of hospitals and the acquisition of medical inputs, such as overpricing, the use of front companies (e.g., a wine store selling ventilators) and bid rigging. *Operation Placebo* was one of the most prominent investigations, targeting Rio de Janeiro's former state governor, Wilson Witzel, which culminated in his impeachment.

Currently, the highest-profile case is the Covid-19 CPI (Parliamentary Commission of Inquiry), which is investigating alleged irregularities in the actions of the federal government and use of public funds in respect of the covid-19 pandemic in Brazil.

2 Outline the legal framework for corporate liability in your country.

Criminal liability is personal and subjective, so that only individuals who have some degree of involvement in a criminal activity may be held liable for it. The exception is environmental crimes. In these cases, there is criminal liability for entities when an environmental crime is committed either (1) as a result of a decision by an entity's legal or contractual

1 Heloísa Barroso Uelze, Felipe Noronha Ferenzini and João Augusto Gameiro are partners at Trench Rossi Watanabe. The authors acknowledge the assistance of senior associates Marlos Corrêa da Costa Gomes and Fernanda Fisher Casagrande, and associates Tiago Caruso Torres and Gustavo Lima Kroger.

© Law Business Research 2021

representative or by its board, or (2) in the company's interests or for its benefit (Federal Law No. 9,605/1998).

In cases not involving environmental offences, corporations or other non-natural persons cannot be charged with crimes but can be held liable for illicit administrative and civil acts. The main legislation regulating corporate liability for illicit acts with a focus on corruption matters is as follows:

- Federal Law No. 12,846/2013 (the Anti-Corruption Law), which came into force in January 2014, deals with the civil and administrative liability of companies for acts against the public administration, whether national or foreign. The Law determines, in Article 2, the strict liability of companies for unlawful acts committed on their behalf, including acts of third parties, with no need to demonstrate the companies' knowledge or intent.
- Federal Law No. 8,429/1992 (the Administrative Improbity Law) establishes the administrative and judicial liability of legal entities and individuals whose actions are to the detriment of the public administration and public interests, resulting in illicit enrichment, losses to the public treasury or violation of the public administration's principles, such as morality.
- Federal Law No. 8,443/1992 (the TCU Law) subjects the contracts entered into with the public administration to the review of the Federal Court of Accounts (TCU). At the federal level, the TCU is responsible for overseeing contracts with the federal administration and imposes penalties if any damage is caused to the public treasury (e.g., caused by fraud in a public tender).
- Federal Law No. 14,113/2021 (the New Public Biddings and Contracts Law), establishes general rules for bidding and administrative contracts. Regarding administrative offences and sanctions, this Law includes reference to violation of the Anti-Corruption Law and now provides for more objective criteria for cases of debarment and associates certain types of conduct to certain time ranges for the debarment. Furthermore, this Law adds a new chapter (IIB, Articles 337-E to 337-P) to the Criminal Code, specifically concerning crimes relating to public bidding and administrative contracts. Law No. 8,666/1993 (the former Bidding Law) already provided for some criminal acts; however, Law No. 14,133/2021 has a more punitive effect, in view of the increased penalties stipulated.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

There is multiplicity of sanctioning authorities in Brazil, whose competence is attributed by different laws, which causes some legal uncertainty for companies.

First, there are authorities legitimised by the Federal Constitution for ensuring administrative morality and combating acts that harm the public administration, including acts of corruption, and fraud in public bids and contracts. Article 129, III of the Constitution establishes that the Public Prosecutor's Office is responsible for protecting public and social assets and hence is competent to file the related lawsuits for acts harming them. Article 70 of the Constitution determines the duties of overseeing public contracts by

© Law Business Research 2021

the Federal Court of Accounts and its related competence to review the use of public resources and initiate administrative proceedings in the event of violations.

Under the Anti-Corruption Law, the highest authority within a public entity (in executive, legislative and judiciary branches) who has been affected by an act of corruption is allowed to investigate, start an administrative proceeding and impose administrative sanctions. In relation to the federal executive branch and foreign public administration, the Law establishes that the Office of the Federal Comptroller General (CGU) has authority to investigate, process and sanction illegal acts set forth in the law.

Under the Administrative Improbity Law and New Bidding Law, a public entity that has suffered the damage may investigate and initiate an administrative proceeding. The Public Prosecutor's Office is also competent to initiate a judicial proceeding for violation of these laws in respective federal, state or municipal branches.

In addition, other authorities have power to enforce rules relating to specific legal areas, such as the Administrative Council for Economic Defence, which enforces antitrust violations, and the Securities Commission (CVM), which enforces rules relating to publicly traded corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The authorities must be aware of minimum elements of the occurrence of a violation to initiate an investigation. However, it is not necessary to have certainty about the occurrence of a violation or about the individuals responsible for it.

From the perspective of the Anti-Corruption Law, following Normative Instruction 13/2019, as amended by Normative Instruction 15/2020, the CGU, or any other competent authority that has obtained information about an alleged violation, may decide about the admissibility of the claim and whether there is sufficient evidence to initiate a preliminary investigation.

According to a Brazilian Supreme Court precedent, no criminal prosecution can be initiated based only on an anonymous report or information provided in leniency agreements with no documentary evidence.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Individuals and legal entities may challenge a notice or subpoena by filing a preliminary defence or injunction before the administrative or judicial court. Depending on the matter, a habeas corpus or an injunction may be filed before superior courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

As of 2019, Brazilian criminal law allows individuals and companies to benefit from a non-criminal prosecution agreement. Non-prosecution agreements (NPAs) are applied to companies only in respect of environmental crimes, which are the only crimes for which legal entities can be held criminally liable.

© Law Business Research 2021

NPAs can be proposed by the public prosecutor in relation to crimes for which the minimum penalty is imprisonment for up to four years. As part of the NPA, the legal entity must repair the damage caused as a result of the offence, carry out community service and pay a fine. The public prosecutor may also impose other obligations on that legal entity.

In June 2020, the Federal Public Prosecutor's Office released Soft Law (*Nota Técnica*) No. 1, published by the 5th Coordination and Review Chamber – Combating Corruption, which permits individuals to subscribe to leniency agreements that are entered into by prosecutors with corporations as a means of co-operation.

Also, the Anti-Crime Law (Law No. 13,964/19) has made it possible for the defendants in an improbity lawsuit to negotiate civil NPAs.

7 What are the top priorities for your country's law enforcement authorities?

The main priorities for law enforcement authorities continue to be in respect of acts of corruption (including bribery, fraud, money laundering and administrative misconduct); however, the spotlight, which had been focused on *Operation Car Wash*, is now on the public measures taken in response to the covid-19 pandemic.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

The Anti-Corruption Law provides that the adoption of compliance programmes by legal entities may reduce the applicable fines by up to 4 per cent (from a fine that be up to 20 per cent of gross revenue). The Law's Regulating Decree No. 8,420/2015, in Article 42, establishes the parameters for compliance programmes to be considered effective.

The CGU provides guidelines about the implementation of effective compliance programmes for private companies and the parameters used to evaluate compliance programmes by means of the 'Integrity Programme Evaluation Handbook for Administrative Accountability Procedures'.

Further, some states are enacting legislation requiring compliance programmes for companies that enter into public contracts with those states. The New Bidding Law provides that a compliance programme will be mandatory for large contracts (over 200 million reais) and will be a tiebreaker criterion for other contracts.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Brazil has approved its Data Protection Law, which requires data controllers and data processors to adopt security, technical and organisational measures to protect personal

© Law Business Research 2021

data against unauthorised access and from accidental or illicit destruction, loss, alteration, communication or any other inappropriate or illicit processing. The imposition of fines has only been allowed since August 2021, so trends in enforcement of cybersecurity-related failings are yet to develop.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Brazilian law includes specific norms against cybercrime activities. Other norms may apply to illegal activities conducted via the internet, software or hardware (e.g., terrorism, crimes against intellectual property of computer software, crimes against children and teenagers, crimes against honour, racism and xenophobia).

As a rule, cybercrimes are investigated by the state police departments. However, the Federal Police is specifically empowered to investigate (1) terrorism crimes, (2) crimes involving misogynistic activity, or internet activity that amounts to hatred of or an aversion to women, and (3) crimes that have a transnational characteristic, all of which Brazil is committed (via international treaties) to combat and prevent.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The Criminal Code sets forth the requirements for applying Brazilian criminal law to crimes that have occurred abroad (from start to finish) (Criminal Code, Articles 7 and 8). Brazilian jurisdiction has extraterritorial effect in two possible situations.

The first of these relates to genocide (when the offender is Brazilian or is living in Brazil) and crimes committed against:

- the Brazilian president's life or freedom;
- public trust;
- property owned by public administrative bodies, companies owned by public administrative bodies or public foundations; and
- the public administrative body, including crimes against an individual who is acting on behalf, or under the orders, of a public administrative body.

The second situation requires different conditions to be applied according to the type of crime, including crimes that Brazil is obliged to repress based on an international treaty or convention, or crimes committed by Brazilian individuals or in Brazilian aircraft or vessels (commercial or private) in a foreign territory if no other court decision on its merits has been issued.

Finally, Brazilian law applies to crimes that occur in public vessels and aircraft, vessels and aircraft used for public purposes, and private vessels and aircraft (on the high seas or in Brazilian airspace).

© Law Business Research 2021

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Brazilian authorities both co-operate on criminal matters with foreign authorities and request the co-operation of foreign authorities. Co-operation between authorities can involve the execution of acts relating to the collection of evidence (interviews, breach of bank secrecy, etc.), transfers of convicted individuals and freezing of assets, among other things, during criminal investigations or lawsuits.

Brazil has multilateral and bilateral co-operation agreements with several countries. If there is no existing agreement with a particular country, it is possible to enter into a mutual settlement for future situations.

Thus, situations vary depending on the relationship and legislation of other countries. The main challenges faced in cross-border investigations are (1) the time spent waiting for other countries' answers or proceedings, (2) the necessary observation of formalities to ensure that evidence collected abroad will be considered valid in Brazil (not null or illicit), (3) certain restrictions imposed by relevant data protection laws (e.g., Swiss Law), (4) blocking statutes and (5) situations for which Brazil does not have an existing agreement.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy is not generally permitted under Brazilian criminal law. Exceptions apply regarding the extraterritorial effects of genocide (when the offender is Brazilian or is living in Brazil) and crimes against (1) the Brazilian president's life or freedom, (2) public trust or property owned by public administrative bodies, or companies owned by public administrative bodies or public foundations, or (3) public administrative bodies, including crimes against an individual who is acting on behalf of an administrative body (see question 11).

However, regarding civil and administrative liability, the coordination of the competent enforcement authorities is a relevant issue. In fact there are several authorities legitimised for filing administrative and civil proceedings and applying sanctions for corruption acts. In addition, the wording of the Anti-Corruption Law's does not clearly resolve the question of legitimacy and the coordinated actions of these legitimised parties. The issue is the object of disputes before the courts and what we have seen increasingly are attempted institutional understandings between the enforcement authorities to avoid such questions.

In relation to leniency agreements, Brazil has made some progress. A co-operation agreement regarding leniency agreements was executed on 6 August 2020 by the Federal Comptroller General, the Federal Attorney General, the Ministry of Justice and Public Security and the Federal Court of Accounts for mutual co-operation between the agencies

© Law Business Research 2021

and flow of information and documents within the leniency agreements, allowing comprehensive negotiation that involves all legitimised agencies and hence preventing any further penalties in addition to those provided by the agreement.

14 Are 'global' settlements common in your country? What are the practical considerations?

Brazilian legislation has no clear arrangement regarding global settlements. Nevertheless, a significant number of global settlements have involved Brazilian companies and, therefore, the participation of Brazilian authorities. Recent cases of global settlement have involved Technip and Samsung Heavy Industries.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Foreign authorities' decisions do not determine Brazilian authorities' decisions. There is independence and sovereignty for both investigations and decision-making, even on the same matter. However, a decision by a foreign authority that has assessed the same facts and evidence can be used by the Brazilian authorities as an additional argument for decision-making, since the evidence analysed abroad has complied with the conditions for lawfulness provided for in Brazilian legislation.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

In terms of economic sanctions, the Head Minister of the Federal Comptroller General has signed 15 leniency agreements stating the payment to the Treasury by sanctioned companies of more than 15 billion Brazilian reais (as at June 2021), including fines and reimbursement of damages. Further, according to the Brazilian Transparency portal, at the federal level, Brazilian authorities have barred more than 14,000 companies (as at 26 August 2021) from entering into contracts with public administration authorities.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The level of enforcement action has increased dramatically during the past decade, with 15 leniency agreements and sanctions totalling more than 15 billion reais. During the covid-19 pandemic, Brazilian authorities have continued to be very active. According to the data in the Transparency portal, the number of sanctions of the Anti-Corruption Law has doubled between 2019 and 2021, and the values have increased from 10 million reais in 2019 to 171 million reais in 2021.

© Law Business Research 2021

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Brazil has signed several co-operation agreements with enforcement agencies in countries such as Chile, Switzerland and the United States. Although Brazilian legislation has no clear arrangement regarding global settlements, a significant number of global settlements have involved Brazilian companies and, therefore, the participation of Brazilian authorities.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Brazil has not enacted any blocking legislation. However, Article 17 of the Introductory Act to the Rules of Brazilian Law sets forth: 'The laws, acts and sentences of another country, as well as any declarations of will, will not be effective in Brazil when they offend national sovereignty, order and good morals.' This means that depending on the nature of the foreign decision, its enforcement in Brazil may be challenged.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Brazil has not enacted any blocking legislation. Nevertheless, the Brazilian Civil Code, in Article 15 of Law No. 13,655 (the Introductory Act to the Rules of Brazilian Law), provides for the following:

> *In Brazil, a sentence imposed abroad, which meets the following requirements, will be enforced: a) the sentence was delivered by a competent judge; b) the parties have been served or legally verified in absentia; c) res judicata applies in addition to the necessary formalities for execution in the place where it was given; d) the proceedings have been translated by an authorised interpreter; e) the sentence has been approved by the Federal Supreme Court.*

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct most often come to the attention of companies through:

- whistleblowers;
- hotlines;
- external and internal audits;
- interviews with company executives;
- internal controls;
- enforcement authorities' investigations (subpoenas, search and seizure, and inquiries); and
- news published in the media.

© Law Business Research 2021

INFORMATION GATHERING

22 Does your country have a data protection regime?

The Data Protection Law was passed in August 2018 and is effective from 27 August 2020, although sanctions are allowed only after August 2021.

The Law was inspired by the EU General Data Protection Regulation. It defines 'personal data' as data relating to an identified or identifiable individual and provides for principles such as transparency, purpose, data minimisation and accountability when processing activities take place. Data controllers are required to have a legal basis for processing personal data, and must implement security measures to prevent unauthorised access to or processing of personal data. It also regulates international personal data transfers.

Failure to comply with the law may result in application of warnings, fines of up to 2 per cent of the group's net revenues in Brazil in the preceding year, suspension of processing activities and even a ban on processing data, among other things. There are also privacy principles and related rules established in the Civil Code, the Consumer Defence Code, the Internet Law and other pieces of legislation, all of which will coexist with the Data Protection Law once it is fully effective.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Intervention by law enforcement authorities has been limited mostly to cybersecurity failings involving breach or unauthorised processing of consumer-related personal data. To the extent that sanctions are imposed, the authorities have so far applied the sanctions established in the Consumer Protection Code, not those in the Data Protection Law.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

There are many precedents in Brazil concerning an employee's privacy rights in the workplace and in the context of an employment relationship. Privacy and data protection concerns may arise if a company fails to clearly communicate to employees its policies in connection with monitoring employees' activities, technological resources, use of personal devices for employment-related activities and so on.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Interception of employees' communications has been regulated through precedents of the labour courts in Brazil. The general rule is that employees should not have any expectation of privacy when using resources offered by the employer for employment-related activities. This position is strengthened if the employer establishes clear policies on the monitoring of employees' activities in the workplace and the use of company-provided resources.

© Law Business Research 2021

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Recent major criminal investigations (e.g., *Car Wash*, *Zelotes*, *Greenfield*, and those relating to covid-19) show that search warrants and dawn raids have been the preferred mechanism for public authorities to collect evidence more quickly and effectively. Under Brazilian criminal law, the police must present a specific search and seizure warrant, duly authorised by the court, to a particular department of the company or for material pertaining to certain employees. General searches inside company premises are not allowed. If authorities exceed the limits of a search warrant, both the individuals and companies involved and affected by the improper collection of evidence can request that any seized documents be retracted and excluded from the case.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Under Brazilian law, attorney–client communication is privileged and confidential. The definition of specific spaces within the legal department and the explicit identification of documents covered by privilege are ways to protect material from being improperly seized during a dawn raid. Even so, an injunction before the courts must be submitted and the material seized must not be used as evidence in the investigation or lawsuit.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Under Brazilian criminal law, individuals who are suspected of involvement in committing an offence cannot be compelled to give testimony. These individuals also have the right against self-incrimination and there is no crime of perjury. Compelled testimonies regarding these individuals are illegal and cannot be used in criminal procedures.

Witnesses, on the other hand, are obliged to collaborate with an investigation. If witnesses do not comply with an order to attend a hearing, they can be sanctioned with a fine, can be coercively conducted to a police station or court, and can be charged with the crime of disobedience.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Federal Law No. 13,608/2018 introduced the concept of whistleblowers to the Brazilian legal system and the importance of their co-operation. The Law provided guidelines

© Law Business Research 2021

for telephone services on receiving complaints and granting anonymity and rewards for information that contributes to the investigation of illegal conduct by private or public organisations.

Law No. 13,608/2018 was amended by Federal Law No. 13,964/2019 (the Anti-Crime Package) in respect of retaliation towards whistleblowers, such as arbitrary dismissal, unjustified alteration of functions and the imposition of sanctions. Any retaliation against whistleblowers will constitute a serious disciplinary offence. The agents of retaliatory conduct may be subject to dismissal from public service and the whistleblower may be compensated twice for any material and moral damage.

In addition, the Anti-Crime Package added, in Article 4-C section 3, the possibility of the whistleblower's participation in up to 5 per cent of the amount recovered by the state.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employment law in Brazil has undergone major changes, but it continues to be protective towards employees. As regards conduct within the scope of an investigation, it is recommended that employees be allowed to defend their actions and counter any accusations.

An investigation must adhere to the required levels of secrecy and discretion to avoid anything being revealed that might cause harm to employees.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

An employee involved in misconduct may be reprimanded or dismissed with cause. In either case, he or she has the right to apply for the matter to be addressed in court.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

No.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

In general, it is good practice to prepare a document that sets out the investigatory scope. This document generally covers questions to be clarified, which mechanisms will be used to achieve those clarifications (e.g., gathering computer records and cell phone data, interviews and background checks), identification of the parties potentially involved, any potential violations of the legislation and authorities with jurisdiction.

© Law Business Research 2021

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Despite not having legal provisions in this sense, as soon as an irregularity is reported, companies must initiate an internal investigation to collect relevant evidence respecting its internal investigation protocols, which should provide the steps to be taken, such as to:

- check whether there are special circumstances, such as senior management involvement or legal violations;
- identify whether there is a need to protect and collect data from the people allegedly involved;
- identify whether there is a need to suspend payments or contracts;
- select people to interview, if applicable; and
- conduct corroboration and financial analyses, if applicable.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

A company should immediately involve its legal team (in-house, external or both) to identify the extent of the allegations, the potential risks, whether other authorities would also have jurisdiction, and which stakeholders should be informed.

The company must respond to the authority in a timely manner, be co-operative, transparent and provide all the information requested, in an accessible format. In the meantime, the company should conduct its own investigation into the allegations.

It is also very important to establish which documents are subject to the attorney–client privilege.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Disclosing an internal investigation is not mandatory. The decision to report the existence of an internal investigation to the law enforcement authorities depends on several factors, including whether the company has shares that are traded publicly.

If a company decides to disclose the findings of an internal investigation, the timing and quality of disclosure should be carefully considered. For example, to fulfil the requirements of a leniency agreement, the company must be the first to contact the authorities and disclose its findings, and provide documents that demonstrate a violation and identify the individuals involved in the offence.

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are currently encouraged by local law enforcement agencies and, in some cases, local authorities request the assistance of internal investigators to structure

© Law Business Research 2021

their cases. However, the internal investigations have to be conducted while respecting constitutional rights – such as the right to remain silent in interviews and to be accompanied by a lawyer if requested – otherwise its use in a formal proceeding could be considered null.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Any communication between an attorney and a client in the context of a representation is protected in Brazil and is not subject to disclosure to third parties, with limited exceptions.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Professional confidentiality is reflected in the Brazilian Constitution as a fundamental right. Within the legal system, privilege rules protect any communication between a lawyer and a client in the context of legal representation. The Brazilian Bar Association's Code of Ethics and Discipline provides that an attorney has a duty to maintain confidentiality of all facts of which he or she has become aware while practising law, including activities of mediation, conciliation and arbitration. The rule makes no distinction between a company and an individual.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The protection of confidentiality applies to the relationship between external attorneys and their clients, and between a company and its in-house counsel, as long as the communication is about legal matters. Recent regulation from the Brazilian Bar Association has acknowledged that privilege is also applicable to in-house counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

All kinds of legal advice are protected equally under the duty of confidentiality. The attorney must maintain the confidentiality of facts learned during the practice of his or her profession. The term 'facts' also includes information disclosed in the exercise of any typical legal activities, such as those described in Article 1 of Law No. 8,906: consulting, advising and legal management.

© Law Business Research 2021

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of the attorney–client privilege may be requested by authorities as part of a plea agreement or a leniency agreement. Usually, at the beginning of settlement discussions, the authorities and the individual or company sign a non-disclosure agreement to protect the information that will be shared in the context of the negotiation. After the agreement is signed, a waiver may be included in the resolution.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no specific regulation covering the extension of a waiver or the prohibition of a limited waiver. Note that legal proceedings in Brazil have a different level of secrecy and, in some instances, the docket case file may be deemed entirely confidential at the court's discretion.

It is possible to waive privileges for only certain forms of communications.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Clients may claim limited waiver in Brazil and thus privilege may be claimed over information provided from another country.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Under Brazilian law, the concept of joint defence does not exist. However, attorney–client communications are protected by the broad confidentiality principle. In recent cases, courts have stated that the duty of confidentiality is extended to the client, but only to people who have a common interest in the facts being investigated, including potential co-defendants.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

According to Provision 188/2018 (Articles 4 to 6) of the Brazilian Bar Association, a lawyer conducting an investigation can directly take all the investigative steps necessary to clarify the facts, in particular collecting testimonies, researching and obtaining data and information available from public or private agencies, determining the preparation of expert reports and examinations, and performing reconstructions, except in the event that a member of the judiciary has exclusive jurisdiction over the matter.

© Law Business Research 2021

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Provision 188/2018 of the Brazilian Bar Association provides for a defensive investigation conducted by lawyers in defence of their clients. Article 4 of this Provision authorises lawyers, when conducting defensive investigations, to directly take all investigative steps necessary to clarify the facts, especially at witness interviews. Note, however, that application of this Provision is restricted to the practice of law in the context of defensive investigations.

On 24 August 2021, the Full Council of the Brazilian Bar Association approved a Provision, already in effect, with the aim of consolidating the prerogatives of legal professionals, so that, when exercising consultancy, advisory, management and legal direction positions in companies, lawyers may use all the rights described in the statute. The approved provision regulates Article 7 of the statute.

Companies may regulate the investigative steps, including interviews, but constitutional rights shall be granted to employees, such as the rights to remain silent and to be accompanied by a lawyer.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Provided an attorney was involved in the process, privilege may be claimed.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Brazilian legislation has no provision in this regard. Nevertheless, it is advisable to indicate that the content of the interview is privileged and that the witness should regard the matter as confidential.

It is essential that the interviewer starts by making clear the investigation is being conducted in the interests of the company. Therefore, confidentiality belongs with the company, which will be informed of the content of the interview to assist with the investigation.

Employment contracts are governed by the general principle of good faith, which imposes on the parties duties of loyalty, information and mutual respect.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Typically, the lawyer conducting the investigation should have a list of questions and documents to be shown as evidence to a witness. Employees, if they so wish and at their request, may have their own legal representation at the interview.

In general, there are two types of interviews: overview and confrontational. Overview interviews can be conducted at any time during an investigation (usually at the beginning)

© Law Business Research 2021

and aim to provide elements to better prepare the investigation team to understand the facts being investigated.

Confrontational interviews usually occur after the document analysis. These interviews must be organised in advance: a list of proposed questions will be drafted and the evidence to be submitted to the witness for clarification will be gathered. It is also recommended to establish in advance, when possible, whether any relevant disciplinary action will be necessary, so that human resources and IT staff can be available (to formalise dismissal or to collect corporate devices, etc.)

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Reporting misconduct is not mandatory in Brazil. In fact, there is an established constitutional principle that establishes the right not to incriminate oneself.

However, if a company or individual wants to enter into a leniency agreement or plea agreement, co-operation is required. Companies interested in entering into a leniency agreement with the Brazilian authorities must be the first to come forward and collaborate to identify the others involved in the administrative infraction.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Prior to self-reporting, it is highly recommended to identify which authorities are likely to have jurisdiction over the matter and contact them all (although this is a difficult task to coordinate), to mitigate any risk of legal uncertainty in connection with a subsequent investigation and to avoid any lawsuits being initiated by other authorities on the basis of the information reported to a specific authority.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

First, the self-reporting entity should ensure that sufficient evidence has been obtained (usually via an internal investigation) regarding facts that may still be unknown by the authorities or about which there is a lack of evidence. The entity should also ensure that it has completely ceased to be involved in the harmful act. It should then identify which are the relevant competent authorities. It may be necessary for the entity to carry out an assessment of the self-reporting requirements for each authority. Initial contact may be made with authorities to provide preliminary information, by executing a non-disclosure agreement. It is important for a self-reporting entity to be supported by experienced lawyers during these negotiations.

© Law Business Research 2021

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Some authorities are open to being approached by companies and may agree to initiate discussions on a possible settlement. Some companies also choose to instruct a local lawyer to make the first approach without disclosing the company's name. Other authorities are more restricted and may not agree to provide any information to companies. In the latter case, companies may claim access to investigative proceedings in court.

55 Are ongoing authority investigations subject to challenge before the courts?

Any individual or company under investigation may challenge proceedings in a court if any rights are violated. The challenge may be broad, such as to terminate the investigation, or limited, with respect to a specific act or piece of evidence.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Brazilian and foreign authorities are in constant communication and have shared relevant information in many cases. Thus, it would be advisable to retain counsel in all countries that may be involved in the enforcement actions. Counsel should decide the best strategy in each case and, if possible, should initiate communications with all authorities at the same time. It is also recommended that transparency and isonomic relationships are maintained with all the authorities.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, a company must search for and produce any material requested by the authorities. If the material or documents are located in a country with restricted privacy laws, the company must retain local counsel and report the legal conflict to the authorities. In certain cases, to avoid local claims, the foreign authorities should request production of the document directly to a local authority and not to the company.

© Law Business Research 2021

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

As has been seen during the *Operation Car Wash* investigations, the Brazilian authorities have shared and received information from several authorities, including in the United States and Switzerland. Brazil has signed bilateral co-operation agreements with several other countries, including Chile and Switzerland, and has ratified international agreements such as the Palermo Protocols and the US Foreign Account Tax Compliance Act.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

In December 2019, the Plenary of the Supreme Federal Court approved the sharing of taxpayers' banking and tax data obtained by the Federal Revenue and the Financial Intelligence Unit with the Public Prosecution Office and the police authorities, without the need for prior authorisation from the judiciary.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The scope for Brazilian authorities to request documents is limited to the jurisdiction of Brazil, unless it has made a formal request to the foreign authority, which would have to accept the request and make the formal request for the foreign company.

If the production of a certain document or piece of evidence encounters any restriction or impediment in the legislation of the other country, the company may refuse to provide it, on the grounds that the production of the document or evidence would constitute a violation of the legislation of the other country.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

According to Brazil's Data Protection Law, companies and individuals may retain information about other individuals or companies only if supported by particular requirements. It is not yet clear how the law will be implemented.

Approval from the Superior Court of Justice for the enforcement of international decisions or subpoenas is necessary. This type of decision or subpoena will not be deemed valid and enforceable if it violates Brazilian sovereignty.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

There is no particular risk with voluntary production. Considering that co-operation may result in a reduction of sanctions in the context of Federal Law No. 12,846/2013 (the Anti-Corruption Law), companies may consider voluntary disclosure. Once produced (voluntarily or compelled), the material may be discoverable if there is no requirement to maintain secrecy in the case.

There is no particular confidentiality in the production of material, but a company may request secrecy in respect of all material or business-related information. In a voluntary production under a leniency agreement, there are confidentiality rules, and evidence has to be returned to the company if a settlement is not reached.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Following conviction, penalties that may be applied to individuals (including company officers and directors) are imprisonment, restriction of rights and fines.

Federal Law No. 12,846/2013 (the Anti-Corruption Law) establishes administrative and judicial sanctions for violations of its provisions, as follows:

- Administrative sanctions:
  - fine ranging from 0.1 per cent to 20 per cent of the gross revenue of the legal entity in the fiscal year prior to the initiation of administrative proceedings, excluding taxes, which shall never be lower than the advantage obtained and never greater than three times the advantage, when it is possible to estimate it; if it is not possible to use the gross revenue criteria, the fine will be between 6,000 and 60 million Brazilian reais; and
  - publication of the condemnatory decision.
- Judicial sanctions:
  - loss of assets, rights or valuables representing, directly or indirectly, the advantage or benefit gained from the infringement;
  - partial suspension or interdiction of the legal entity's activities;
  - compulsory dissolution of the legal entity; or
  - a ban on receiving incentives, subsidies, grants, donations or loans from public agencies or entities, and from public financial institutions or institutions controlled by the government, for between one and five years.

Under the Federal Law No. 8,429/1992 (the Administrative Improbity Law), those who commit a dishonest act against the public administration are subject to administrative sanctions, such as loss of assets obtained from the wrongdoing (disgorgement), full damage compensation, removal from public function and loss of political rights (for individuals), a ban on receiving incentives, subsidies, grants, donations or loans from public

© Law Business Research 2021

agencies or entities for up to 10 years, a fine of up to three times the value of the undue advantage, and a ban on contracting with the government for up to 10 years.

Federal Law No. 8,443/1992 (the TCU Law) provides that the applicable fines may be up to 100 per cent of the updated value of the damage caused to the treasury.

Federal Law No. 14,113/2021 (the New Public Biddings and Contracts Law) provides for sanctions in the form of fines and bans on bidding and contracting, such as the declaration of ineligibility to bid or contract for up to six years (which is longer than the two years provided for in the previous law).

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

From a criminal perspective, settlement in another country does not prevent a company (or its directors) from being held criminally liable in Brazil. In view of the co-operation between authorities, information presented to a foreign authority can potentially be shared with Brazilian authorities and, therefore, expose the company to civil and administrative liability and its directors to civil and criminal liability in Brazil. Therefore, if co-operation with another country is envisioned, the company may also consider the benefit of a simultaneous settlement in Brazil.

65 What do the authorities in your country take into account when fixing penalties?

Brazilian courts should follow three steps to determine the penalties that will be imposed on an individual. In the first instance, the court should consider:

- the individual's culpability, criminal background and social behaviour;
- the motivation for the crime, the circumstances and the consequences; and
- the conduct of the victim.

Second, the severity of penalties should be increased in consideration of:

- recidivism by the offender;
- the motivation for the crime;
- how the crime was committed;
- who the victim is;
- the behaviour of the offender during the crime;
- the context in which the crime was committed; and
- the leadership of the offender.

Conversely, penalties may be reduced in consideration of:

- admission of guilt by the offender;
- the offender's age;
- the motivation for the crime; and
- any attempt by the offender to mitigate the consequences of the crime.

© Law Business Research 2021

As a third step, the court should consider general or specific criteria – depending on the crime in question – to increase or decrease penalties (e.g., attempted use of a firearm).

In relation to fines, criminal law prescribes certain parameters. In addition, the financial situation of the offender should be considered in applying an appropriate penalty.

The Anti-Corruption Law provides aspects that shall be taken into consideration when applying sanctions to legal entities, which are:

- the seriousness of the infraction;
- the advantage obtained or intended by the offender (or offenders);
- the fulfilment or not of the infringement;
- the degree of injury or the risk of injury;
- the negative effect produced by the infringement;
- the economic status of the legal entity;
- the level of co-operation by the legal entity in the investigation of violations;
- the existence of internal mechanisms and procedures for integrity, auditing and incentive to report irregularities and the effective application of codes of ethics and conduct within the scope of the legal entity; and
- the value of the contracts maintained by the legal entity with the injured public body or entity.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Non-prosecution agreements (NPAs) can be proposed by the Public Prosecutor in relation to crimes for which the minimum penalty is imprisonment for less than four years. As part of the NPA, the beneficiary must repair the damage caused as result of the offence, carry out community service and pay a fine. The Public Prosecutor may also impose other obligations on the company.

The company is entitled to this benefit if it is not a recidivist and has not benefited from an NPA in the past five years. Once the conditions are accepted by the company, the agreement will be ratified by a judge.

Under Federal Law No. 12,846/2013 (the Anti-Corruption Law), companies may enter into a leniency agreement to resolve a case of corruption administratively. In relation to companies, the Anti-Corruption Law defines rules for any leniency agreement between the highest authority of each public agency or entity and companies. An effective collaboration from the companies may reduce the applicable fine by up to two-thirds.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Reporting restrictions or anonymity for companies are determined in each leniency agreement to ensure the effectiveness of the collaboration and the useful outcome of the

© Law Business Research 2021

lawsuit. In general, to ensure fairness in these proceedings, a proposed leniency agreement will not be announced to the public until after the agreement is effective or after the district attorney's office presses charges against the defendants.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies should investigate to establish whether there is evidence of the irregularity, the involvement of the company, whether elements could be useful to the authorities and the potential benefits of the settlement.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

There is no legal provision regulating the use of external monitors, although this tool is now being used in Brazil, such as in the *Odebrecht* case. In 2019, TechnipFMC signed an agreement with the authorities, with provision for compliance monitoring by members of the Federal Comptroller General.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Third parties may file an indemnity or contractual judicial claim and a court or authority may decide to provide access to third parties.

In the event of a claim for indemnity by a minority shareholder, there are some precedents of court decisions denying this right on the grounds that the action against the controlling shareholder must be promoted by the company, and that the minority shareholder cannot claim against the company for indirect losses, since the individual action is only applicable in the event of direct loss.

Regarding requests for documents and information about agreements, companies may claim the attorney–client privilege to refuse to supply documents and information to shareholders, as well as in view of the confidentiality and secrecy of the evidence produced, except in the event that it is possible to prepare a summary report in which the main issues are dealt with in the agreements and are public knowledge.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

A police investigation is generally public. However, an investigation may be conducted in secret when it is necessary for the police to ensure the effectiveness of the investigation or to protect the identity of a suspect or victim. Individuals under investigation and their attorneys are entitled to have access to the records of the investigation, except any measures that are still being conducted (e.g., searches and seizures that are still being prepared or ongoing wiretapping). It is a crime in Brazil to deny a lawyer, or an individual under investigation, access to the investigation files.

© Law Business Research 2021

Criminal lawsuits are also public, unless secrecy is necessary to protect the privacy or identity of the defendant or victim.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for larger companies to use external public relations companies, and publicly traded companies make use of their internal investor relations departments. These are the most common options for handling external communications.

73 How is publicity managed when there are ongoing related proceedings?

Administrative accountability procedures (known as PARs) conducted by the Federal Comptroller General publicise the name of a company that is subject to a sanction. Once a company is sanctioned, that decision is also made public.

Information about several confidential cases in Brazil has been leaked.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

This should be assessed in each case, but is mainly dependent on whether the matter involves a publicly traded company, in which case the company has a duty to disclose material information regarding its business and finances as they relate to the settlement.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

There is no legislation regulating ESG matters. However, during the anti-corruption compliance process, among the preparatory acts for mergers and acquisitions, customers have begun to seek confirmation of compliance with corporate, environmental, labour governance and anti-corruption compliance in their due diligence procedures, in addition to specific technical analyses.

Normative Ruling No. 586 from Brazil's Securities Commission (CVM), which amended Normative Ruling No. 480, obliges publicly held companies to report on the adoption of governance practices according to the Brazilian Corporate Governance Code. The disclosure to the market or the delivery to the CVM of information that is false, incomplete, inaccurate or that induces the investor to error, as well as failure to comply with the submission deadline, are considered serious infractions and may be sanctioned with penalties.

© Law Business Research 2021

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

The CVM launched a public hearing on 7 December 2020 in respect of possible changes to CVM Rule No. 480/09 with the aim of improving the rules about requirements regarding disclosure of ESG matters by publicly traded companies in Brazil.

Federal Law No. 14,113/2021 (the New Public Biddings and Contracts Law) also provides relevant updates from an ESG perspective; for example, national sustainable development is one of the main goals of public tenders. Within the concept of sustainability, future projects should consider aspects such as reverse logistics, low energy consumption and accessibility. Among other main points addressed by the new law in respect of ESG, it will also provide incentives in relation to governance, risk and compliance practices. The integrity programme will have a relevant role in public contracts, as it will be mandatory in large contracts, a tie-breaker criterion in the bidding process, an element to be considered in the definition of sanctions and a condition for rehabilitation of sanctions.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Companies are obliged to disclose employment information and work conditions to the respective relevant labour unions and class entities.

Although no disclosure is required, and in Brazilian jurisdiction there is no criminal liability for companies in this regard, a company's administrators may be criminally liable on a personal level if they have been involved in acts of slavery or racism, among others.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Bill of Law No. 2,505/2021, which has the aim of making changes to Federal Law No. 8,429/1992 (the Administrative Improbity Law), may have knock-on effects and is being criticised for creating obstacles to enforcement. Among the potential changes are the limitation of the time for an investigation to be concluded, a reduction of the statute of limitation and restrictions on cases allowing assets to be frozen, among others.

© Law Business Research 2021

8

Chile

Alex van Weezel and Santiago Breton[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Currently, the *Corpesca* case is the highest-profile corporate investigation under way in Chile. It concerns Corpesca SA, a Chilean fishing company, and two politicians, former senator Jaime Orpis and former congresswoman Marta Isasi.

The investigation began in the context of a political scandal about illegal financing of electoral campaigns by large businesses that arose in 2015. The scandal affected politicians from all sides of the spectrum and involved prominent Chilean companies, such as SQM, Penta and Corpesca. The criminal case involves charges for bribery, fraud against the public treasury and tax evasion offences.

In 2018, Chilean prosecutors filed criminal charges against former senator Orpis, former congresswoman Isasi and Corpesca. The trial ended in December 2020. The court found Mr Orpis and Mrs Isasi guilty of fraud against the public treasury and bribery offences. It also found Corpesca guilty in connection with those crimes.

Remarkably, Corpesca is the first Chilean corporation that has been criminally charged and sentenced, despite having asserted a compliance programme defence during the prosecutor's investigation and subsequent trial.

Therefore, once it is finally over, the *Corpesca* case will probably set forth the first judicial standards for the corporation's compliance defence in Chile. There are currently several appeals for annulment pending that will be heard by the Chilean Supreme Court.

1 Alex van Weezel is a partner and Santiago Breton is an associate at Claro y Cia.

© Law Business Research 2021

2 Outline the legal framework for corporate liability in your country.

Law No. 20,393, enacted in November 2009, established for the first time a criminal liability regime in Chile for legal entities. This Law punishes companies if certain criminal offences are committed in their interests or benefit by their owners, managers or chief executives, provided that those crimes are a consequence of companies breaching their supervision duties. In practice, companies can avoid criminal liability if, before the execution of the relevant crime, they have designed and implemented an effective compliance programme to prevent these crimes.

Law No. 20,393 operates only under some express established offences. Initially, this list included only bribery, money laundering and financing of terrorism. However, since its enactment, the Law has been amended to expand a corporation's criminal liability to other underlying offences, such as certain environmental crimes, some forms of corporate fraud and, most recently (in mid-June 2020), crimes against public health (relating to the covid-19 crisis).

The Congress is currently discussing Bill No. 13.205-07, which significantly expands the list of offences for which legal entities can be held criminally liable, along with other relevant changes to the current regulation of corporate liability, such as (1) an expansion of the number of crimes for which legal entities are criminally responsible, (2) modifications to the requirements for allocating liability to them, (3) changes to conditions required for a compliance programme to exempt them from liability, among other things.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The primary enforcement authorities that regulate corporations in Chile are the Commission for the Financial Market (CMF), the Internal Revenue Service (SII), the Antitrust Prosecutor's Office (FNE) and the Criminal Prosecutor's Office (MP).

Each office has jurisdiction over its own subject matter, but the MP centralises all criminal enforcement competences. Notwithstanding the above, there are certain crimes (such as tax evasion and cartel offences) that can only be criminally prosecuted if the relevant technical office (e.g., the SII or FNE) first files a formal criminal complaint.

In general, each office has internal guidelines or protocols relating to the prosecution of corporations. For example, the general criteria for the criminal investigation and prosecution of corporations under Law No. 20,393 are established in the National Prosecutor's General Instruction No. 440/2010.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

As a general rule, an enforcement authority can open and conduct an investigation either at its own initiative or at the request of a third party. However, Chilean law does not generally establish a threshold of suspicion to trigger an investigation. Although each agency usually has protocols to guide these decisions and allowing their control, they are usually subject to a discretionary decision-making process.

© Law Business Research 2021

In any case, there are certain offences (such as cartel and tax evasion offences) that can be prosecuted by the MP only if the technical authority (e.g., the FNE or SII) has requested it to do so by filing a criminal complaint.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

As a general rule, private parties must comply with subpoenas to produce documents. However, if the materials requested are protected by legal confidentiality rules (for example, banking transactions records), the party can in practice refuse to comply with the subpoena until a court authorises the seizure of the requested materials.

Private parties are also generally forced to comply with subpoenas to give testimony. In criminal investigations, witnesses can only refuse to answer a given question based on the privilege against self-incrimination, incrimination of a close relative or professional secrecy.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Leniency or immunity agreements have been introduced in some particular areas during the past decade, especially relating to corporations. Two of the most important are the leniency programmes of the CMF and the FNE. Both grant immunity or lesser charges to whistleblowers who actively co-operate with the authority's investigations relating to certain breaches against financial markets or antitrust regulations. Likewise, whistleblowers are entitled to a reduction of the criminal penalties that they can face for the same facts.

However, the law does not provide a general regulation about leniency agreements in criminal cases. Nevertheless, if a defendant (including corporations) makes significant contributions to the investigations, prosecutors might consider it a mitigating circumstance and apply to the judge for a reduction in penalties. In respect of certain crimes (e.g., corruption crimes and some forms of organised crime), the law mainly regulates their implementation by prosecutors and judges.

7 What are the top priorities for your country's law enforcement authorities?

In recent years, the authorities have prioritised enforcement actions against major corporations, for corruption, antitrust and, lately, environmental violations.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Under Law No. 20,393, a corporation cannot be held criminally liable for a relevant offence committed in its interest or for its benefit if, before the event occurred, the company has

© Law Business Research 2021

designed and implemented an effective compliance programme. According to Article 4º of Law No. 20,393, an effective compliance programme must have at least the following elements: (1) a compliance officer, appointed by the highest administrative authority of the legal entity, with adequate resources, material means and power to carry out the role; (2) a risk-based crime prevention system, that is to say internal protocols, rules, procedures and sanctions, to adequately prevent the commission of relevant offences in the context of the company's areas of activity; and (3) a mechanism to monitor, assess and update the company's crime prevention system, and to detect and correct its flaws.

The Chilean Congress is currently discussing Bill No. 13.205-07, which could simplify these requirements. If the Bill is passed, a compliance programme would have to meet the following requirements: (1) identification of the legal entity activities that imply a risk of criminal conduct; (2) establishment of protocols and procedures to prevent and detect that type of conduct, which must consider safe channels for reporting complaints; (3) assignment of subjects responsible for the application of these protocols, endowed with effective powers of direction and supervision; and (4) periodic evaluations and mechanisms for improvements or updates. All the foregoing would be subject to the the legal entity's resources, complexity and activities.

To date, courts have not analysed the extension and material content of an effective compliance programme, except for the *Corpesca* case, which is still ongoing. Further, the MP has not addressed this matter in General Instruction No. 440/2010, which sets forth the general criteria for the criminal investigation and prosecution of corporations under Law No. 20,393.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Law No. 19,628 on Personal Data Protection governs the management and treatment of personal data and databases. In general, according to this law, the treatment and management of personal data, defined as any information relating to specific or identifiable individuals, must be authorised by law or expressly in writing by the owner of the information (data subject), whose authorisation may be revoked (with no retroactive effect) at any time. The data subjects must be duly informed as to the purpose for which their personal data are collected and about the potential disclosure of the data to the public. All personal data must be used exclusively for the purpose for which it was collected. This law establishes a general duty of care on those responsible for databases (both controllers and processors): these parties shall take care of the data with due diligence and are also responsible for any damage. Moral and compensatory damages can be claimed before an ordinary civil court.

Law No. 19,628 on Personal Data Protection does not have specific provisions on cybersecurity, such as obligations to report security incidents or specific data security requirements. A Bill currently in Congress at an advanced stage (Bill No. 11.144-07) does include the duty to adopt safety measures and reporting obligations in regard to security breaches (e.g., the duty to report any security breach to the Personal Data Protection Agency by the most expeditious means possible and without undue delay).

© Law Business Research 2021

When a breach affects sensitive data, the data controller must inform the data subjects of the breach in clear and simple language, specifying the data affected, the possible consequences of the security breach and the measures adopted to avoid further damage, among other things. As the Bill has not progressed in the Congress very quickly, and in the absence of regulations, other authorities have started to react to privacy issues, such as the National Consumer Bureau (SERNAC) on consumer protection and the Commission for the Financial Market (CMF) in respect of regulations on cybersecurity issues.

SERNAC

Law No. 19,496 on Consumer Protection, in the context of e-commerce, includes provisions regarding the security of websites and apps: a website or app must have the technical features to provide security and confidentiality to personal and financial data provided by consumers, considering events such as alteration or unauthorised transfer of that data, unauthorised disclosure, or interception or malicious access by third parties. These security measures relate mainly to the redirection to secure sites under the cryptographic protocol 'https' and the verification of the padlock symbol in the web browser, without confusing security images, among other things. Both the website or app and the means of payment offered must have a high standard of computer security and the user should be informed about this.

This Law also considers a voluntary procedure for the protection of collective interests (collective mediation) and subsequent class action lawsuits following security breaches. SERNAC is actively seeking compensation for consumers who have been affected by security breaches, such as disclosure of personal information, interruption of computer services, limiting users to carry out their transactions, in addition to causing other damage, including duplication of charges and differences in balances in checking accounts. The proceeding can only begin if no class actions that relate to the same facts have been filed and, once the proceeding has commenced, no class actions can be filed concerning the same facts until the voluntary proceeding ends. This proceeding can be initiated by SERNAC or following a complaint from a consumer's association.

CMF

This public entity has issued several regulations on cybersecurity for banks and financial institutions. The main provisions seek to raise security standards and to obtain accurate information about security breaches quickly.

The obligations of banks and financial institutions to report cybersecurity incidents to the CMF include a 30-minute limit for reporting the first information about any incident; entities must inform any event of relevant operational incidents affecting business continuity, information security or the image of the institution. CMF regulations also set minimum conditions that must be considered for the development and maintenance of information regarding cybersecurity incidents. A digital platform has been established by the CMF for incidents to be reported to the regulator within 30 minutes. Additionally, there is an obligation to appoint a manager at executive level to communicate with the CMF at all times (Chapter 20-8 of the Updated Compilation of Rules (*Recopilación Actualizada de Normas* (RAN)).

© Law Business Research 2021

The handling of cybersecurity incidents by banks or financial institutions is considered a relevant factor to determine their evaluation and classification as financial institutions of higher or lesser rank. There is an obligation to record and have a complete register of all cybersecurity incidents, with a full description of each incident. There must be a framework for action established by the board of directors of the entity, which must consider the specific management strategy for this risk, the level of tolerance admitted, roles and responsibilities of participants, processes and methodologies to be used for its management in consideration of best practices, the volume and complexity of business activities and existing international standards. The board has the obligation to rule on managing cybersecurity at least once a year (RAN, Chapter 1-13).

Regarding operational risks, regulations further require banks to continuously monitor operational risks, to invest in technology and security that mitigate these risks and that are consistent with the volume and complexity of an entity's activities and operations. Entities must have an adequate long-term plan in respect of technological infrastructure, and a structure in place dedicated to managing the security of information in general and cybersecurity in particular, business continuity plans and contingency (RAN, Chapter 1-13).

Also, the CMF regulations contain general guidelines regarding outsourced services, in particular the outsourcing of data processing services and additional safeguards in the case of cloud services. The provisions set the conditions that an entity must meet before making the decision to outsource a service, including essential requirements regarding the sites of processing, aspects of business continuity and information security, among other things. Regarding this last aspect, the bank must require the supplier to ensure confidentiality, integrity, traceability and availability of the information assets (RAN, Chapter 20-7).

Finally, and related to the latter topic, there is a special regulation on bank fraud. Law No. 20,009 allows cardholders to limit their liability with respect to transactions subsequent to the notice of theft, robbery, loss or fraud that must be given to the issuing institution. They may even be exempted from liability for transactions prior to such a notice if they are allegedly unaware of having consented to or given authorisation for such transactions. This regulation of limited liability protects not only cardholders but also users of other electronic transaction systems.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Law No. 19,223 establishes the primary cybercrime offences in Chile to protect data and computer systems. However, its provisions are very outdated, as this Law has not been amended since its enactment in 1993, causing significant difficulties to Chilean prosecutors in prosecuting and obtaining convictions for these types of crimes. Therefore, law enforcement authorities have prioritised the prosecution of cybercrime under general offences that are committed using computer systems (e.g., fraud).

In May 2020, Congress passed Law No. 21,234, which amended Law 20,009 to establish several types of fraud relating to misuse of banking cards and electronic fund transfers made through the internet (e.g., phishing). The Law also allows the implementation of relevant and sensitive investigative techniques, such as interception of communications, controlled delivery and undercover operations, among other things. The Chilean Investigations Police (PDI) has a specialist department to investigate cybercrime matters.

© Law Business Research 2021

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

As a general rule, Chilean criminal law is governed by the territorial principle. However, Article 6 of the Organic Code of Courts establishes those exceptions for which criminal law will have an extraterritorial effect; for example, when Chilean people or individuals with their habitual residence in Chile bribe a foreign official abroad, or cartel offences that affect the Chilean market, and when Chilean officials commit certain corruption crimes abroad (e.g., tax fraud and bribery). Similarly, Law No. 19,913 on Money Laundering lays down another exception under Article 27, which enables punishment in Chile for a money laundering offence, even when the relevant predicate offence was committed abroad.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Some law enforcement agencies have specialist departments to handle international co-operation, such as the International Cooperation and Extraditions Unit (UCIEX) of the Criminal Prosecutor's Office (MP) or the Financial Analysis Unit (UAF). Each unit has signed its own international agreements with foreign authorities to improve cross-border investigations. Hence, difficulties arise when an investigation involves a country with which enforcement agencies have not signed an agreement; in these cases, co-operation will mainly depend on the other country's interest and willingness.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

In general, Chilean law does recognise the criminal judgments made by foreign courts (Code of Criminal Procedure, Article 13). Thus, in principle, corporations shall not be criminally prosecuted and punished in Chile on the same set of facts on which they were convicted or acquitted abroad. However, Chilean law shall not recognise double jeopardy if it appears that the aim of the first trial was to avoid prosecution under Chilean courts, or that the first trial was conducted in a way that either violates due process guarantees or in any other way reveals a lack of intention to judge the defendant genuinely.

Chilean law does not have a general provision concerning multiple law enforcement authorities seeking to penalise, as with the United States' anti-piling on policy. The Chilean Constitutional Court has given some guidelines on this matter but its case law is still unclear. Initially, the Court established that the double jeopardy principle applied to the sanctioning powers of administrative agencies (STC 244-1996). However, during

© Law Business Research 2021

the past few years, the Court has expressly refused to apply the double jeopardy principle in cases relating to securities offences investigated in different countries, arguing that the infringement affected different markets, among other reasons. As a consequence, this is a matter that must be considered case by case.

14 Are 'global' settlements common in your country? What are the practical considerations?

No, they are not common in Chile.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

The decisions of foreign authorities are typically just another piece of evidence for an investigation, without any special effect provided by Chilean law. However, in practice, they can influence how Chilean authorities are likely to evaluate the merits and strengthen of their own cases.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Chilean law has not implemented a sanctions programme, similar to those adopted and enforced by the United States, the United Nations (UN) and the European Union.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Since Chile does not have a sanctions programme, local authorities do not have an enforcement approach in this matter. However, since Chile is a member of the United Nations, local authorities seek to comply with the economic sanctions imposed by the Security Council Sanctions Committees. For example, the Financial Analysis Unit (UAF), the Chilean specialist agency on money laundering, monitors UN sanctions to detect money laundering offences in Chile and to co-operate with foreign authorities.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Although Chile has not implemented a sanctions programme, agreements signed by several local institutions can allow them to co-operate with foreign authorities in charge of sanctions compliance and enforcement. For example, that could be the case with the UAF, for which one of the primary purposes is to co-operate with foreign financial entities to prevent and detect money laundering and the financing of terrorism.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Not that we are aware of.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

They usually come to light through self-reporting in the context of a company's internal investigation, whistleblowing and media reports. Also, during the past few years, the use of social media has become increasingly important in this respect.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Yes. Law No. 19,628 governs the management and treatment of personal data and databases by private and public entities.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Chile does not have a specialist data protection agency. Therefore, the enforcement of data protection provision under Law No. 19,628 is mainly addressed by courts in the context of civil suits that seek compensation for possible violations of data protection rights. Nevertheless, a Bill that creates the Personal Data Protection Agency is currently being discussed in the Chilean Congress. If the bill of law is passed, the Agency will be responsible for ensuring compliance with the rules on the processing of personal data and its protection.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The most pressing issue is the general lack of regulation, which has caused a certain degree of uncertainty on the limits of an employer's rights and powers when conducting internal investigations. For example, there is no clarity on the limits of digital discovery through an employer's information technology systems (e.g., employees' emails). Although these systems are the employer's property, it is not clear whether the employer can freely search and use an employee's communications as part of an internal investigation because they can contain private information about the employee.

© Law Business Research 2021

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no regulation in this respect. Nevertheless, case law from the labour courts and the Labour Department have provided some criteria. As a general rule, there is an expectation of privacy in respect of employees' communications (including emails) under the Chilean Constitution, which protects them through intimacy rights and inviolability of communications guarantees. Thus, any interception of employees' communications by employers, without prior employee consent, would be banned. Sometimes employers seek to address this limitation in employment contracts, but local courts have questioned the validity of such agreements regarding non-business-related communications.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes. As a general rule, search warrants and dawn raids must be authorised by a judge. Usually, the law requires the authority that is conducting the investigation (for example, a prosecutor in a criminal investigation) to provide grounds for the possible infraction that is under investigation, and to state the necessity and utility of the warrant for the success of the investigation. Typically, the warrant must be executed by the public officials designated by the judge in the order, within a set time provided by the judge, and after the affected party is properly notified of the warrant. Authorities are required to maintain strict custody of, and record, all seized items.

In criminal investigations, Article 220 of the Code of Criminal Procedure bans authorities from seizing all communications, or documents and notes about them, of the defendants with their close relatives or their lawyer. In respect of a defendant's lawyer, the prohibition is extended to the offices or premises where the lawyer works.

If the authorities exceed the limits fixed by the law, companies can ask a judge to consider that the evidence obtained is null and should be excluded from the trial. Companies might also file a constitutional complaint so as to cease any excessive behaviour based on a violation of fundamental rights.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

As a general rule, the law does not establish a special mechanism to protect privileged material during a dawn raid or when the relevant enforcement authority is executing a search warrant that has been authorised by a judge. Thus, in practice, the only way to protect privileged material would be by opposing the seizure of items during a dawn raid or by refusing to fully comply with the search warrant, based on its privileged nature, and later trying to challenge the warrant (or limit its scope) in court.

© Law Business Research 2021

In criminal investigations, the defendants can request a hearing to discuss how the seizure of those items affects constitutional due process guarantees and, consequently, their constitutional right to a defence. At this hearing, the defendants could request that the judge order the return of any privileged material that has been seized by authorities.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

All private parties must respond to a summons and give testimony to authorities in their own proceedings. Otherwise, they can be compelled to do so by the courts – typically, the courts will impose a fine or issue a warrant for the arrest of non-compliant parties. Exceptionally, private parties can refuse to answer a particular question if there is a risk of self-incrimination, incriminating close relatives or breaching their professional secrecy duties (e.g., the attorney–client privilege). Also, in criminal investigations, defendants cannot be forced to give testimony; they can use their constitutional right to remain silent. Finally, persons with diplomatic immunity only testify on the basis of a written report, if they voluntarily consent to do so.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Chile does not have a particular regulation regarding whistleblowing proceedings within a company. However, pursuant to Article 4 of Law No. 20,393, an effective compliance programme must include, among other elements, an adequate and effective channel for the company's employees and agents to report improper conduct.

In practice, financial incentives for whistleblowers are not common in Chile.

Finally, according to Chilean labour case law, employers must take appropriate measures to guarantee that their internal investigation proceedings respect and protect the employee's constitutional rights to privacy, honour and due process, among other things.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

The law does not explicitly grant special rights for employees whose conduct is under the scope of an investigation. However, under Chilean labour case law, these proceedings should always respect due process guarantees and employees' constitutional rights. Otherwise, disciplinary measures taken by a company against implicated employees (e.g., suspension or dismissal) might be refused by a judge. In this regard, employment law does not distinguish between employees, officers and directors.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

As a general rule, during an investigation, an employee who is suspected of misconduct retains the same primary labour rights that are available to all other employees. Thus, for example, the employer may not stop paying his or her salary. However, the employer should take appropriate action to prevent further misconduct by the same employee. For example, in cases of sexual harassment, the employer must take measures to protect the injured party, which could include the possible suspension of the implicated employee while an investigation is under way. The precautionary measures that an employer can take will depend on each particular case. In any event, the measures must be proportional to the investigated misconduct and the fundamental labour rights of the employee (such as due process guarantees).

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Only if the employee has voluntarily accepted in his or her contract (or in another mandatory internal regulation) that he or she will participate, co-operate and testify in internal investigations. In this situation, an employee who refuses to participate in an internal investigation will be in breach of contract, which provides a legal ground for dismissal.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

There is no general standard or common practice on these matters. However, during the past few years, it has become increasingly common for internal investigations to be conducted within major corporations. In these situations, the documentation will usually identify the main parties involved in the inquiry (the claimant and the accused), a summary of the facts and the basic procedural terms, such as deadlines during the investigation, its phases and the investigator in charge.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

As a general rule, the law does not force companies to report misconduct to the authorities. However, in some cases, self-reporting could be advisable. For example, to obtain the legal benefits established by a leniency programme (e.g., of the Commission for the Financial Market (CMF) or the Antitrust Prosecutor's Office (FNE), the law usually

© Law Business Research 2021

requires the provision of sufficient information to the authorities regarding a possible infraction. Generally, to meet that requirement, it is necessary to carry out an internal investigation and to collect the evidence that will be presented to the authorities at a later stage.

Notwithstanding the above, companies are required by law to investigate any allegation of sexual harassment and to provide the results of that investigation to the Labour Department.

Finally, when an issue involves a listed company, reporting up or briefing the board could be a necessary step to comply with basic corporate governance rules. The decision to take this step will depend on the nature of the issue and must be evaluated in each case.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Companies are generally required to comply with notices or subpoenas that seek to produce documents of which the companies have custody. Although the law does not regulate the steps a company should take to comply with this type of request, it is advisable to adopt reasonable measures to collect and preserve the documents that are in the company's possession at the time it receives the notice or subpoena. Individuals who deliberately destroy or alter documents requested by authorities can face criminal charges under obstruction of justice provisions (e.g., Article 269 *bis* of the Criminal Code and Article 7 of Law No. 19,913). The criminalisation of this type of conduct is becoming increasingly common in Chile (e.g., Article 39(b) of Law Decree No. 211).

Further, some administrative agencies (such as the CMF and the Internal Revenue Service (SII)) can impose sanctions on people who destroy relevant documents and cause difficulties in executing the auditing powers of those entities.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

As a rule, it is not mandatory for companies to disclose an internal investigation to law enforcement authorities. Nevertheless, it is relevant for companies to evaluate the benefits of self-reporting in the case of leniency programmes, such as those established for investigations conducted by the CMF or the FNE. In that regard, it would be advisable to disclose evidence and to contact the relevant authorities.

When an issue involves a listed company, reporting up or briefing the board could be a necessary step to comply with basic corporate governance. This decision must be evaluated case by case. However, if the issue in question is deemed to be material information (i.e., what a prudent man would consider important for his investment decisions), the law obliges public offer issuers registered with the Securities Register to disclose the information to the public in a truthful, sufficient and timely manner (Law No. 18,045, Securities Market Act, Article 9).

© Law Business Research 2021

37 How are internal investigations viewed by local enforcement bodies in your country?

As long as they do not interfere with local enforcement investigations, internal investigations are welcomed, especially if their results are later shared with the authorities.

Regarding sexual harassment allegations, companies are required by law to conduct internal investigations and share the results with authorities. In other types of cases, sharing internal investigations with authorities can allow a company to obtain a legal benefit (e.g., an attenuating circumstance under Law No. 20,393) or can be a requirement to gain access to a leniency programme.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

The law does not explicitly address this matter. However, there are certain provisions, both civil and criminal, which, when interpreted in the light of due process, make it possible to argue that the attorney-client privilege can be invoked to protect the content of internal investigations from disclosure.

Thus, in civil matters, it is not possible to order the exhibition of documents that 'have the character of secret or confidential'. In addition, the law allows the production of certain documents to be requested as a preliminary injunction, but only to the extent that, by their nature, they may be of interest to different persons, which would exclude documents covered by the attorney–client privilege (Code of Civil Procedure, Articles 349 and 273).

On the other hand, in criminal matters, a judge cannot apply measures of constraint to force lawyers to hand over means and documents that are in their possession and that refer to aspects covered by the attorney–client privilege (Code of Criminal Procedure, Articles 217 and 303), nor order the seizure of communications, notes, objects or documents to which the power to refrain from giving testimony 'naturally' extends (Code of Criminal Procedure, Article 220).

Furthermore, the Chilean Bar Association has been particularly clear in pointing out that seizures of documents protected by professional secrecy are not acceptable, neither are court orders that disregard the existence of this privilege.

Based on the above, it is possible to develop a typology of objects or documents that are produced and collected in an internal investigation that should be protected by the attorney–client privilege, especially considering the constitutional guarantees of due process and right to a defence.

To protect the privilege or confidentiality of an internal investigation, it would be highly advisable to state explicitly the protected nature of the communications and documents that are part of the investigation (e.g., by labelling them as confidential, attorney work-product or privileged), and also to state the involvement of a lawyer in

© Law Business Research 2021

the investigation. In addition, the custody of these documents could be entrusted to the respective lawyer to prevent intrusions or unwanted access.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Chilean law does recognise the attorney–client privilege but it does not define it or state its key elements or principles. However, the Chilean Bar Association's Code of Ethics provides the following general principles on this matter, without making any distinction between individual clients or corporate clients:

- the only person who can consent on the disclosure of a client's secrets is the client;
- prohibition on disclosure: lawyers cannot disclose to third parties a client's confidential information or facilitate access to the documents and other materials in which that information is contained. Lawyers can, or must (depending on the case), reveal confidential information without the consent of the client only in exceptional and grave circumstances (for example, to prevent a felony being committed). In any case, disclosures are always subject to strict filters of necessity and proportionality;
- duty of care in respect of all information received or disclosed: lawyers must take reasonable steps to secure the confidentiality of the client's information;
- duty of care towards those who assist an attorney: lawyers must adopt measures to guarantee that those who collaborate with them will maintain the client's confidentiality; and
- the client's confidentiality must be maintained indefinitely, even after legal service.

Finally, the attorney–client privilege is recognised by the Code of Criminal Procedure as an exception to refuse to answer particular questions on criminal proceedings. The seizure of communications between a lawyer and a client is also prohibited, including the notes or documents referring to the client. Likewise, Article 231 of the Criminal Code punishes with fines and temporary (or even permanent) debarment those lawyers who abuse their position by disclosing their clients' secrets. Finally, the Code of Civil Procedure does not authorise requests for the production of secret or confidential documents and also exempts lawyers from the obligation to testify on facts that have been communicated to them in confidence (Articles 273, 349 and 360).

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

It could reasonably be argued that the attorney–client privilege applies equally to both in-house and external legal counsel since the law does not make any distinction between them. In this regard, Article 220 of the Code of Criminal Procedure bans the seizure of communications (and documents that contain communications) between a defendant and a lawyer by prosecutors, extending that privilege to the premises where the lawyer works.

Notwithstanding the foregoing, it should be noted that in a recent decision of the Competition Court (TDLC), it was decided not to exclude from the file certain documents containing transcripts of communications between company executives and lawyers.

© Law Business Research 2021

According to the Court, this was because the passages referring to communications with an external lawyer who conducted an internal audit had been blacked out; however, the court apparently considered that the passages referring to communications with the in-house lawyer were not covered by the attorney-client privilege, because it did not order that they be blacked out or excluded from the file. Nevertheless, this is an isolated ruling that does not amount to case law and should therefore be analysed with caution.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

There is no regulation or official guideline on this issue yet. Even though the law and the Chilean Bar Association's Code of Ethics does not make any distinction in this regard, it is unclear whether a court will recognise the attorney–client privilege in respect of foreign lawyers who are not legally authorised to practise in Chile.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There are no contexts in which waiving the attorney–client privilege is mandatory or required as a form of co-operation. Further, enforcement authorities will not automatically deem those who refuse to waive the attorney–client privilege as unco-operative.

Co-operation credit is always an issue that is evaluated by authorities in each case. In this regard, authorities can deem that an individual who is voluntarily waiving the attorney–client privilege is effectively co-operating with an investigation conducted against that individual. As a rule, only clients can free their lawyer from their duties of confidentiality.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The concept of limited waiver of privilege does not exist in Chile.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There are currently no laws, case law, regulations or guidelines that address this matter.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privileges does not exist in Chile.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

According to the Chilean Bar Association's Code of Ethics, lawyers must take reasonable measures to guarantee that those who collaborate with them will maintain a client's

© Law Business Research 2021

confidentiality. However, it is not clear that those collaborators can claim any privilege over their work, or that lawyers can claim that their attorney–client privilege is extended to, or covers, the work performed by those collaborators.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Chilean law does not regulate this type of procedure. However, it is common practice for employees or other witnesses to be interviewed as part of internal investigations.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

This matter is not explicitly addressed by Chilean law. However, it can be argued that a company could claim the attorney–client privilege over attorney reports, as long as the facts that are under investigation entail a risk of criminal liability for the company itself. In that situation, the company could claim that those documents are protected by Article 220 of the Code of Criminal Procedure, which forbids the seizure of notes or reports that are drawn up by attorneys and give an account of the communications between a defendant and an attorney.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There is no specific regulation on this issue. However, companies should consider guidelines provided by labour case law, according to which, when conducting internal investigations, employers must respect their workers' constitutional rights. They should avoid threats, coercion and retaliation against employees who refuse to testify. Also, they should guarantee that employees testify voluntarily and secure the confidentiality of employees' testimony.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Companies usually design their own internal investigation procedures; these can vary depending on the size of the company and the complexity of the matter involved. Typically, a specially designated member of the company (or sometimes a committee) will interview possible witnesses and review relevant documentation.

Interviews are generally conducted under confidentiality conditions. Depending on the complexity of the case, relevant documents might be put to the witness for further clarification.

© Law Business Research 2021

Legal representation for employees is not mandatory nor a common practice. If an employee wants to have his or her own attorney present during an interview, the company will decide whether to grant this request based on due process guarantees.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

As a general rule, reporting misconduct to law enforcement authorities is voluntary. Exceptionally, the Code of Criminal Procedure mandates public officials and directors of private clinics and educational institutions, among others, to report offences of which they become aware while performing their functions (Article 175).

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting would be advisable when a company can access a leniency programme, for in these cases, the company could obtain an exemption or a reduction of its sanction. This happens with certain violations investigated by the Commission for the Financial Market (CMF) (infractions to securities or insurance regulations), the Antitrust Prosecutor's Office (FNE) (cartel offences) and the Superintendency of the Environment (environmental violations). However, each case must be evaluated separately; the same criteria apply to extending self-reporting to another country.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Self-reporting has become increasingly common in Chile since the CMF and the FNE created regulations for accessing a leniency programme. Generally, it is important to collect and provide sufficient evidence regarding the infraction. Likewise, companies are usually prevented from disclosing that they have applied to a leniency programme. In practice, companies submit a brief to the authorities, describing the infractions and presenting the evidence they have collected. As a general rule, to obtain the benefits provided by the leniency programme, it is necessary to self-report before authorities open an investigation into the company.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Responses to subpoenas are usually made by submitting a letter to the authorities providing the required information.

© Law Business Research 2021

The option to enter into dialogue with the relevant authority before answering a subpoena depends on a variety of conditions, such as the nature of the proceeding, the position the company holds in the investigation, the nature of the information requested, and the severity or urgency of the subpoena, among other things. For these reasons, this possibility needs to be assessed case by case.

55 Are ongoing authority investigations subject to challenge before the courts?

Usually, they are not. However, in criminal investigations, judges can review specific investigative measures adopted by prosecutors or police, to control whether they meet the standards required by law. In those cases, the judge will oversee particular acts, but it would not be possible to challenge the whole investigation.

In addition, the Code of Criminal Procedure (Article 186) allows any person affected by a 'non-formalised' investigation to request a judge to order the prosecutor to report on the facts under investigation, and the judge may even set a deadline for the prosecutor to 'formalise' the investigation. Nevertheless, in Chile it has been interpreted that entitlement to this right is available only to the defendant.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

It is not common for companies in Chile to receive subpoenas or notices directly from foreign enforcement authorities. These requests are always processed via local authorities. For this reason, companies should seek to respond to multiple subpoenas consistently. If that is not possible given the conflicting terms of the subpoenas, it would be advisable to try to negotiate a consistent disclosure package, with either local or foreign authorities.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

As a general rule, companies must respond to subpoenas by providing the requested documents that are in their custody. The law does not force companies to seek and collect information that is not in their possession to comply with a subpoena.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Currently, Chilean law enforcement authorities frequently share information with foreign agencies. In fact, in the case of criminal investigations, the Criminal Prosecutor's Office (MP) has a special department (the International Cooperation and Extraditions Unit

© Law Business Research 2021

(UCIEX)), which has signed several co-operation agreements with authorities from other countries relating to criminal prosecution. The UCIEX unit coordinates all foreign information requests.

Likewise, national agencies, such as the CMF, the Internal Revenue Service (SII) and the Financial Analysis Unit (UAF), also have co-operation units and their own international conventions for this purpose.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Generally, authorities must keep their proceedings secret from third parties and allow access only to interested parties. Several legal provisions establish secrecy duties for public officials who work in law enforcement agencies, regarding information they access in their official capacity. A breach of those duties usually entails criminal liability for the official involved.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The law does not force companies to seek and collect information that is not in their possession to comply with a subpoena from authorities. For that reason, in such a case, it would be advisable to respond to the subpoena by stating that the company does not have the requested documents in its custody.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Chile does not yet have secrecy or blocking statutes.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Chilean law does not make any difference between voluntary or compelled production of documents. However, compelled production of material will usually entail a risk of a dawn raid by authorities.

As a general rule, documents collected by authorities will be kept secret from private third parties while the investigation is current. However, once it has been completed, the documents could be subject to public information requests. Should that be the case, authorities will disclose them if the affected party does not refuse disclosure on the basis that it would affect their safety, privacy or commercial or economic rights.

© Law Business Research 2021

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Chilean law usually punishes individual misconduct with imprisonment, fines and bans to perform a profession or activity.

In the case of a company's criminal liability, Law No. 20,393 establishes the following penalties:

- dissolution of the entity;
- a ban on entering into acts or contracts with the state either permanently or for an established period;
- partial or total loss of fiscal benefits;
- fines; and
- forfeiture of the benefits received as a consequence of the felony committed.

Congress is currently discussing Bill No. 13.205-07, which will modify these penalties if it is passed. In essence, forfeiture would be no longer considered as a penalty – even though it will continue to apply – and there would be two new penalties: the supervision of the legal entity and the publication of an excerpt of the condemnatory sentence (under current law the latter is only a facultative penalty).

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Chilean law follows the principle of territoriality. Thus, there are commonly no options or restrictions that are applicable.

65 What do the authorities in your country take into account when fixing penalties?

Fines are the most common sanction for companies, and there is a large degree of discretion within the frameworks established by the law. However, regulations frequently include guidelines that authorities should follow. In general terms, those regulations take into account the severity of the violation, the benefits obtained by the offender and the extension of damage caused to third parties, among other things.

If Bill No. 13.205-07 is passed, a system of daily fines, according to the income of the convicted person, shall be established.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Chilean law regulates an alternative resolution mechanism for criminal cases, known as a conditional suspension of the procedure (CSP), which operates as a deferred prosecution agreement. Pursuant to Article 25 of Law No. 20,393, companies may obtain a suspension

© Law Business Research 2021

of the criminal proceeding for a fixed time (between from six months and three years) if they accept and agree to comply with one or more conditions proposed by the prosecutor and sanctioned by a judge. Those conditions can include paying an amount to the state or the victim, community service, implementing a compliance programme, or any other condition that is suitable to the case. If the company complies with those conditions during the period of suspension, the judge will terminate the criminal proceeding against the company without a conviction. The company can only access this alternative resolution mechanism after the prosecutor has 'formalised' the investigation against the company. In any case, the agreement must be approved by a criminal judge at a special hearing.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

It is not possible to ensure anonymity since deferred prosecution agreements (known in Chile as CSPs) must be requested by a prosecutor, agreed by the defendant and approved by a judge at a public hearing.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Probably one of the most important aspects that any company should consider is the publicity relating to the agreement. According to criminal law, settlements (i.e., CSPs) are always presented to a judge at a public hearing, whereby the facts under investigation and the conditions of the agreement will be made public. In these cases, although there will be no guilty verdict, the public exposure may still damage the company's corporate image.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

External corporate compliance monitors are not regulated in Chile. However, pursuant to Article 25 of Law No. 20,393, in the context of a CSP, it would be possible to request that a company design and implement a compliance programme that includes an external compliance monitor as a requirement of a CSP.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

As a general rule, criminal law allows victims to present criminal complaints and participate in the criminal proceeding with complete access to the prosecutor's files. Likewise, victims can file civil suits against the defendant to be decided in the context of the criminal trial.

© Law Business Research 2021

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

According to the Code of Criminal Procedure (Article 182), investigations are not disclosed to third parties. However, victims, private complainants, defendants and their defence attorneys always have the right to access the file and obtain copies. Exceptionally, the prosecutor can establish the secrecy of certain proceedings or documents for the defendant and the other parties for a maximum of 40 days.

Once a case is before a court, judicial hearings are always public unless a judge rules to the contrary for specific and duly grounded reasons (Article 289).

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In most cases, a company's internal and external communications are handled by a managing director or a communications manager. Since the internet and social media have become an essential part of companies' public relations, many companies have also appointed social media managers. Nevertheless, in times of crisis (frequently relating to criminal investigations), it is increasingly common for larger businesses to hire an external public relations firm to improve the control of the media and avoid severe reputational damage.

73 How is publicity managed when there are ongoing related proceedings?

There are no common standards in this respect. In practice, corporations usually try to minimise public exposure, even when there are current related proceedings.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Pursuant to Law No. 18,045, only listed companies have to disclose to the market all material information relating to them that might ordinarily be relevant to investment decisions. Therefore, if a settlement is considered to be this type of information by the company's board, they should inform Commission for the Financial Market (CMF).

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Laws No. 18,045, on securities markets, and No. 18,046, on corporations, establish that companies and issuers of public offerings must provide certain information to the public. The Commission for the Financial Market (CMF), by means of General Standard (NCG) No. 30, has established the minimum elements that must be included in the annual report through which such information is to be provided to the public.

© Law Business Research 2021

One of those elements concerns social responsibility and sustainable development, and includes the diversity of directors, managers and workers (gender, nationality, age and seniority) and gender pay gaps. In this way, the information provided covers differences at the board, management and general organisational levels. In addition to the annual report, the entity must also complete an electronic form referring to that same information. This regulation was incorporated in 2015 through a modification introduced by NCG No. 386.

Also, regarding corporate governance, NCG No. 385 contains a questionnaire in which entities must declare whether or not they have adopted certain measures and, if they have not adopted them, they must explain why. This is traditionally known as 'report or explain'. Contrary to the previous case, it is not yet mandatory to include this information in the annual report.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Yes. In April 2021, a consultation process was completed on new regulations issued by the CMF to modernise and improve the ESG information that issuers of publicly traded securities registered in the Securities Register must submit in their annual report. The proposal contemplates a restructure of the current annual report, incorporating ESG issues throughout, in addition to the inclusion of the corporate governance matters referred to in NCG No. 385.

Although the new ESG regulations (i.e., the obligation to inform in the annual report) have not yet been approved, they are structured on the basis of an approach that begins with the entity's governance, strategy and risk management system, which is complemented by the disclosure of specific indicators and objectives. Thus, the annual report should include a profile of the entity, information about its corporate governance and strategy, data on the diversity and conditions of people who work there, information about the business model and the management of its suppliers, a summary of the relevant events that occurred during the respective period, and the comments made by shareholders and directors, financial reports, etc. In particular, indicators of energy and water consumption, and legal and regulatory compliance, should be reported. In addition, there is a requirement for information about ESG indicators according to the type of industry of the entity, according to standards and recommendations established by the Sustainability Accounting Standards Board or the Task Force on Climate-Related Financial Disclosures.

In this way, the information required from the entities is going to be systematised and incorporated in the annual report.

The changes will apply not only to publicly traded corporations but also to banks as issuers of publicly traded securities.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Not that we are aware of.

© Law Business Research 2021

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

When reporting in the previous edition, we expected to see an expansion of the scope of criminal liability for legal entities, under Law No. 20,393, because the number of offences that can explicitly entail criminal liability for companies had increased since 2018.

The Chilean Congress is currently discussing a Bill (Bill No. 13.205-07) that, if passed, will greatly change the extent of regulations for criminal liability of legal entities. For example, the number of offences for which legal entities can be held liable would be significantly extended, in addition to changes in the requirements for compliance programmes and significant alterations to the sentencing regime, with the aim of achieving harsher and more dissuasive sentences. The approval of Bill No. 13.205-07 is still pending and subject to modifications.

© Law Business Research 2021

9

China

Kyle Wombolt, Helen Tang and Tracey Cui[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

As widely reported in the international press, Chinese authorities have been heavily focused during the past 12 to 18 months on regulation and enforcement within the country's growing technology industry. For the most part, this has consisted of the introduction of sweeping regulations aimed at curbing the reach and influence of China's technology giants. There have also been a number of enforcement actions and penalties levied against Chinese technology companies. The State Administration of Market Regulation, for example, has imposed fines on a number of e-commerce companies and consumer technology service providers for a range of infringements, including offences relating to unfair competition, consumer rights, labour practices and promoting false product information.

In one particularly high-profile regulatory intervention in June 2021, the Cyberpsace Administration of China barred ride-hailing company Didi Chuxing from registering new users within days of its initial public offering on the New York Stock Exchange, citing breaches of consumer privacy laws.

Activity in China continues to be a strong focus for international, and particularly US, enforcement agencies. China has been the focus of more US Foreign Corrupt Practices Act (FCPA) enforcement actions than any other country since the enactment of the Act in 1977. Half of the FCPA enforcement actions by the Securities and Exchange Commission to date in 2021 have involved conduct taking place in China. In many cases, these US-driven investigations trigger concurrent or follow-on investigations by China's law enforcement authorities and regulators.

1 Kyle Wombolt and Helen Tang are partners and Tracey Cui is an associate at Herbert Smith Freehills.

© Law Business Research 2021

2 Outline the legal framework for corporate liability in your country.

Corporate entities can be held criminally liable for giving bribes to state personnel (and persons closely associated with state personnel), non-state personnel, foreign officials, and state entities and enterprises. Corporate criminal liability generally attaches where the relevant misconduct is an exercise of 'corporate will' (i.e., the decision to engage in misconduct was a group decision or was made by the personnel in charge). For example, in the high-profile prosecution, GlaxoSmithKline was found guilty on the basis that its management encouraged bribery of doctors, hospitals and other institutions for the benefit of the corporate entity.

Amendments to the Anti-Unfair Competition Law (AUCL), which came into force in January 2018, revised the legal framework for civil bribery. Business operators, which includes corporates, can be found liable for civil bribery offences if they bribe individuals or entities to seek transaction opportunities or a competitive edge. Vicarious liability is expressly presumed.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

By virtue of its control over state-owned entities (SOEs), the Communist Party of China (CPC) is an omnipresent participant in the corporate enforcement arena. The CPC established the National Supervision Commission (NSC) in March 2018 under the Supervision Law of 2018 (the Supervision Law). The NSC is China's new 'super graft agency' and enjoys a status close to the cabinet. It has absorbed and extended the investigative and enforcement powers of the CPC's Central Commission for Discipline Inspection. The NSC may detain individuals, interrogate them for up to six months, freeze assets, search premises with a warrant and seize evidence. Moreover, detainees are not entitled to legal advice as the NSC operates outside the purview of the Criminal Procedure Law of the People's Republic of China of 1979 (as amended) (the Criminal Procedure Law).

The NSC's jurisdiction focuses on corruption and bribery by individuals but it is likely that both SOEs and multinational corporations will get caught up in investigations initiated by the NSC, particularly given its ability to call on the services of other law enforcement agencies.

The NSC carries out investigations of suspected bribery by SOEs and state personnel before referring cases for further review and prosecution by people's procuratorates and the Supreme People's Procuratorate. Public security bureaux (PSBs) may assist with the NSC's investigation if the suspected offences include other crimes that fall outside the NSC's investigatory scope but within that of the relevant PSB.

PSBs investigate, via the economic crime investigation units set up within the bureaux, criminal bribery offences that fall outside the investigatory remit of the NSC, fraud, other financial crimes, and crimes relating to food and drug safety. People's procuratorates, as prosecuting bodies, enjoy their own investigatory powers in relation to certain types of crimes (e.g., crimes committed by law enforcement officers that relate to obstruction of justice) but are primarily responsible for prosecutions. According to the Criminal Procedure Law and the Supervision Law, people's procuratorates will prosecute if they

© Law Business Research 2021

are of the view that the facts of a crime have been ascertained, and that the evidence is concrete and sufficient. The authorities have published no policies specifically relating to the prosecution of corporations, although there are thresholds for the investigation of corporates.

Distinct from law enforcement, other bodies exercise investigative, disciplinary and regulatory powers over corporates. For example, the State Administration for Market Regulation (SAMR) investigates potential violations of the AUCL and sanctions civil bribery. It is not unusual for multiple agencies to be involved in a single matter. If relevant and within their jurisdiction, authorities do not generally refrain from pursuing matters simply because the corporate is under investigation by another domestic body.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In practice, the authorities have considerable leeway in initiating investigations, both procedurally and substantively. The NSC in particular enjoys broad investigative powers, with no particular suspicion threshold stipulated in the Supervision Law.

The Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security have issued guidelines that prescribe minimum monetary thresholds for commencing investigations for certain financial crimes, product quality crimes and others, including minimum thresholds for investigations of corporations.

The Criminal Procedure Law contains a general provision that investigative authorities should 'promptly examine the materials provided by a reporter, complainant or informant, or any voluntary confessions by any suspect'. After initial examination and preliminary investigation, if they consider there are facts indicating criminal liability, they should initiate a formal criminal investigation. The Criminal Procedure Law contains no other details on the threshold of suspicion required to trigger a formal investigation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Assuming that the investigating authority is properly authorised to issue the notice, it is unlikely that a person will have a valid ground to challenge a notice, given that the concept of privilege is not recognised under Chinese law. Challenges to procedural issues may be raised but they can usually be resolved through government actions (e.g., issuance of an amended notice with proper authorisation). In addition, even if a person refuses to produce documents, the investigating authority has broad power to search and seize evidence during an investigation.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Whether an individual is granted any leniency or immunity for assisting with authorities is generally a matter left to the discretion of the authority. However, both the Law on Administrative Penalty and the Supervision Law (enacted in March 2018) contain

© Law Business Research 2021

provisions for more lenient penalties to be available when an individual has assisted or co-operated with authorities.

Article 32 of the Law on Administrative Penalty (updated in 2021) provides that lenient or reduced administrative punishments will be provided to those who have gained credit in helping administrative organs to investigate unlawful acts.

Similarly, Article 31 of the Supervision Law provides that the supervision organs may issue a recommendation for lenient punishment when a person actively co-operates with the authorities, takes active measures or otherwise renders significant assistance in cases involving matters of major national interest.

7 What are the top priorities for your country's law enforcement authorities?

Recent cases against corporations highlight corruption, fraud, product safety, tax evasion, money laundering and terrorism financing as the key areas of focus. There has been an increased focus on investigating potential economic crimes in certain sectors, such as the pharmaceutical, technology, financial and construction sectors.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Under the amended AUCL, vicarious liability is expressly presumed for civil bribery committed by employees of business operators. The law places the burden on the employer to prove that an employee's actions were unrelated to seeking transactional opportunities or competitive advantage for the employer.

When the amended AUCL came into effect, the head of the Anti-Monopoly and Anti-Unfair Competition Enforcement Bureau at the State Administration for Industry and Commerce provided an explanation of what might be required for such a rebuttal. His explanation appeared to suggest that vicarious liability can be refuted if a company has evidence to prove that it had taken reasonable steps to comply with laws and regulations, had adopted effective supervisory and monitoring measures, and had not conspired or connived in an employee's misconduct. The Shanghai Regulation against Unfair Competition (effective from 1 January 2021) encourages business operators to establish an anti-commercial bribery programme and specifies that the implementation of the programme would be reviewed in any commercial bribery investigations conducted by the local SAMR.

In recent years, the government has urged Chinese companies to enhance their compliance procedures in light of the increasingly strict enforcement environment and, since 2017, has issued multiple regulatory documents setting out compliance guidelines and codes of conduct for Chinese companies and foreign companies operating in China.

Most recently, a compliance monitoring mechanism in criminal cases was formally introduced by guidance issued on 3 June 2021 by the Supreme People's Procuratorate, the Ministry of Justice, the Ministry of Finance, the State-Owned Assets Supervision

© Law Business Research 2021

and Administration Commission of the State Council, the SAMR and other authorities ('Guidance on Establishment of a Third-Party Monitoring and Evaluation Mechanism for the Compliance of Enterprises Involved in Cases (for Trial Implementation)'). The Guidance proposes that the local people's procuratorates in the pilot cities may decide whether to go through a compliance monitoring process in a case involving economic crimes or duty-related crimes. This monitoring process would involve an independent third party reviewing the company's compliance programme and preparing reports to the local people's procuratorates, which would be taken into account in prosecution and sentencing decisions. The introduction of the Guidance followed the Supreme People's Procuratorate's launch of the pilot programme of 'Corporate compliance non-prosecution reform' in March 2020 when six local people's procuratorates were selected as pilots. In 2021, the pilot programme has been expanded to local people's procuratorates in 10 provinces, including Beijing, Shanghai, Guangdong and Jiangsu.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

The Cybersecurity Law (CSL) is the key legislation regulating cybersecurity. It contains a set of cybersecurity obligations and requires the authorities to take action against companies and management in relation to cybersecurity-related failings. A key regime under the CSL is the Multi-Level Protection Scheme (MLPS), which requires each network operator to be assessed and designated a particular level of security obligations. The MLPS will be implemented through technical standards and a regulation that is currently being drafted by the Ministry of Public Security.

The penalties applicable in the case of a violation of the CSL include an order for rectification, a warning, forfeiture of illegal income, fines, suspension of business, closure of website, withdrawal of operation permit or revocation of business licence. To date, we have seen enforcement actions that focus on warnings, orders for rectification and fines. With the MLPS regime now being established, more enforcement actions are expected.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime is regulated under the Criminal Law of the People's Republic of China of 1979 (as amended in 1997) (the Criminal Law), which punishes:

- illegal invasion or control of computer systems (or providing programs or tools for such);
- destruction of computer systems causing serious consequences;
- refusal to discharge cybersecurity protection obligations despite administrative orders, resulting in serious consequences;
- using information networks to commit certain crimes, such as fraud and the sale of drugs; and
- abetting others in committing cyber-related crimes.

© Law Business Research 2021

These crimes are punishable by fines and imprisonment. In terms of specific offences, China's law enforcement authorities have focused on infringement of personal data and intellectual property, cyberfraud, cybergambling, cyberpornography and online exam cheating. Law enforcement authorities receive many requests for assistance in cybercrime investigations from international agencies, such as Interpol, and counterparts overseas.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, the Criminal Law of the People's Republic of China of 1979 (as amended in 1997) (the Criminal Law) applies when either the act or the consequence of a crime occurs within China. Individuals who commit a criminal act are subject to the Criminal Law if they are located in China, regardless of their nationality, and Chinese nationals who commit crimes outside China are subject to the Criminal Law provided the punishment is more than three years' imprisonment. The Criminal Law applies to companies organised under Chinese law, including joint ventures, representative offices of non-Chinese enterprises and wholly foreign-owned enterprises.

In late 2018, China passed an amendment to the Criminal Procedure Law of the People's Republic of China of 1979 (as amended) (the Criminal Procedure Law) to allow judgment to be delivered in corruption cases when the defendant is absent. The amendment is designed to tackle cases in which suspects escape justice by hiding overseas. The amendment allows prosecutors to proceed with a case if evidence against the suspect is ample and the crime is clear.

The bribery of foreign public officials by individuals and entities was criminalised in 2011 through an amendment to the Criminal Law. This has not been prosecuted in practice.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

In practice, cross-border investigations involving conduct in China are typically triggered by the US enforcement authorities (the Department of Justice or the Securities and Exchange Commission). The principal challenge is how to deal with Chinese laws on issues such as data privacy, state secrets, trade secrets and the absence of privilege, while seeking to co-operate with US enforcement authorities. The movement of evidence from China is particularly problematic. The divergence in both procedural and substantive law in these areas means that what the US authorities expect from a corporate investigation, and what the corporate can do and provide within the purview of Chinese law, are often at odds. This in turn leads to tension between complying with Chinese law and demonstrating co-operation, which is necessary for leniency, deferred prosecution or a declination in the United States.

© Law Business Research 2021

Although challenges are most often encountered in the context of US cross-border investigations, similar tensions may be encountered in relation to other jurisdictions that may be investigating corporate conduct in China.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Chinese law does not expressly recognise the concept of double jeopardy or anything similar, even for domestic criminal proceedings. In fact, under the Criminal Procedure Law, even if a case has been closed, it can be retried if there is new evidence suggesting that the facts relied on in the original judgment or sentencing were incorrect. In practice, it is not uncommon for a defendant to become a suspect again in respect of the same allegations after a court has delivered a not-guilty verdict.

China is also unlikely to recognise the double jeopardy concept in international criminal enforcement actions. Under the Criminal Law, a person may be investigated and prosecuted in China even if he or she has already been tried in a foreign country. Those who have received criminal punishment overseas may be exempted from punishment or receive a mitigated penalty. However, we are not aware of informal negotiation or co-operation to afford corporate defendants relief in the face of enforcement actions in multiple jurisdictions.

There is no system analogous to the US 'anti-piling on' policy.

14 Are 'global' settlements common in your country? What are the practical considerations?

We are not aware of any concluded global settlement involving China.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions made by foreign authorities may be influential for a number of reasons. They may draw the attention of the Chinese authorities to the matter. They may also serve to make the issue newsworthy and therefore exert political pressure on the Chinese authorities to proceed with the matter themselves.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

China does not have a comprehensive sanctions programme in the same way as other jurisdictions, such as the United States. Rather, the legal basis for its sanctions programme

© Law Business Research 2021

is found in a patchwork of laws and regulations. The Foreign Trade Law authorises China to take corresponding measures against any country or region in response to discriminatory measures. It also allows China to take action based on breaches of anti-monopoly or unfair competition laws. The Customs Law and the Regulations of the People's Republic of China on Import and Export Duties (through which China imposes customs duties) also form part of China's sanctions programme. The Ministry of Foreign Affairs issues circulars that serve as the legal basis for other organs at ministerial level to implement United Nations sanctions. Through the Ministry of Foreign Affairs, China also unilaterally threatens or imposes sanctions based on its foreign policy needs. For instance, following China's statement of its intention to sanction US companies involved in selling arms to Taiwan in October 2020, China cut the supply of rare earth to Lockheed Martin and reduced orders from Boeing in August 2021.

The Export Control Law, which seeks to bring China's export control system closer to other regimes, came into force in December 2020. This Law introduces four categories of controlled items – dual-use goods, military items, nuclear items, and other goods, technologies, services and items relating to national security – and any data relating to the aforementioned items, including technical materials. The Export Control Law also provides for the maintenance of a control list of foreign importers and end users that have been found to violate the law. The Export Control Law seeks to bring China's export control rules and enforcement in line with some other jurisdictions that have more comprehensive controls.

On 1 June 2019, the Ministry of Commerce announced the establishment of an Unreliable Entities List, which has been compared to the United States' Entity List. On 19 September 2020, the Provisions on the Unreliable Entities List were approved by the China State Council and immediately came into effect. The Unreliable Entities List restricts the business of foreign entities in China that endanger the sovereignty, security and development interests of China, or suspend normal transactions with or apply discriminatory measures against an enterprise, other organisation or individual of China, in a way that violates normal market transaction principles and causes serious damage to their legitimate rights and interests. Enforcement mechanisms are not yet established but the Provisions provide for these to be set up. The possible measures against foreign entities may include restricting or prohibiting engaging in China-related import or export activities, investing in China, entry into the territory of China, work and stay permits and imposing a fine, among other things.

On 10 June 2021, China enacted the Anti-Foreign Sanctions Law, which took effect on the same date. It appears primarily to target sanctions imposed by foreign states on China's government officials, although the Law also provides flexibility for a much broader scope of application. Notably, the Law provides that the government may issue an anti-foreign sanctions Counter List, and impose countermeasures on individuals and organisations included in the Counter List and their related persons.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

China's approach to sanctions enforcement should be viewed in the context of the broader geopolitical situation, particularly the ongoing trade tensions between the United States

© Law Business Research 2021

and China. Enforcement could increase in light of the Export Control Law, the Unreliable Entities List and the Anti-Foreign Sanctions Law.

As described above, the Export Control Law, the Provisions on the Unreliable Entities List and the Anti-Foreign Sanctions Law provide a high-level framework for an export control and sanctions programme in China, which may lead to an increase in enforcement activity. How these rules are implemented in practice remains to be seen and is likely to depend, to a significant degree, on the prevailing geopolitical climate.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Generally no, unless this would be mutually beneficial.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

In January 2021, the Ministry of Commerce (MOFCOM) issued its Order No. 1 of 2021: Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures (the PRC Blocking Statute). It applies where the extraterritorial application of foreign laws or other measures prohibits or restricts Chinese entities from engaging in normal economic, trade and related activities with foreign entities. The Blocking Statute introduces several measures, including a reporting obligation and a prohibition order. Chinese nationals, legal persons and other organisations are required to make an accurate report to MOFCOM within 30 days of any instance where they face prohibition or restriction by foreign laws or measures from engaging in normal commercial activities with third-country entities. A prohibition order may be issued by the Chinese government to the effect that the relevant foreign laws and other measures (not specified in the statute) should not be recognised, enforced or complied with, if the extraterritorial application of those laws is deemed unjustifiable. Exemptions from compliance with a prohibition order may be possible upon written application. It also grants parties the right to bring a civil claim before a Chinese court and seek compensation for losses caused by the extraterritorial application of the foreign laws and measures that are subject to China's prohibition orders.

The PRC Blocking Statute is similar in nature to legislation in other jurisdictions. Unlike the current EU Blocking Statute, which is specifically drafted to prohibit EU operators (broadly defined) from complying with specific US sanctions, the PRC Blocking Statute establishes only a general framework by setting out a non-exhaustive list of factors to consider in determining which foreign laws should be subject to prohibition. In response to questions regarding which foreign laws will be targeted initially, MOFCOM has stated that the PRC Blocking Statute does not target any specific countries or specific transactions in specific areas, and that the working panel will keep a close eye on the extraterritorial application of relevant foreign laws and measures.

Notwithstanding these comments from MOFCOM, and although the PRC Blocking Statute does not provide for the publication of a list of specific sanctions regimes or

© Law Business Research 2021

foreign laws, prohibition orders issued in due course will be made publicly available, effectively creating a *de facto* list of 'unjustifiable' foreign laws. It is not clear from the PRC Blocking Statute whether exemptions will be made publicly available.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

In the absence of specific guidance on the applicability or any cases, it remains to be seen whether, and to what extent, the compliance will be enforced in practice.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Whistleblower reports (either internally to a compliance officer or colleague, or externally to a regulatory or enforcement agency) often trigger allegations of corporate misconduct. Internal audits may also identify misconduct. To a lesser extent, complaints by competitors, which may be channelled through media reports, can also cause allegations of misconduct to surface. Inspections by external bodies such as the State Administration for Market Regulation or regulatory authorities may also flag issues.

INFORMATION GATHERING

22 Does your country have a data protection regime?

China's data privacy regime has been evolving quickly, conferring broader rights on data subjects and imposing ever more regulation on companies operating in China. The primary laws regarding data protection consists of the Cybersecurity Law (CSL), the PRC Data Security Law and the PRC Personal Information Protection Law. The CSL, which came into force in June 2017, was the first attempt to harmonise China's data privacy laws. Prior to the CSL, data privacy rights had been arranged in a patchwork of legislation (including Criminal Law of the People's Republic of China of 1979 (as amended in 1997), General Rules of the Civil Law and Tort Law) and in industry-specific regulations (e.g., the banking, healthcare and securities sectors).

The CSL's data protection provisions cover any data that is generated, collected or processed in China by network operators – this covers both domestic companies and multinational corporations. Data collection must comply with relevant laws and regulations and be for a legitimate and necessary purpose. Consent of the data subject to data processing is required. The Personal Information Security Standards (of which the latest version is effective from 1 October 2020) provide best practice guidelines on data protection, which serve as a reference for both users and the authorities. The PRC Civil Code, which came into force on 1 January 2021, contains additional personal information protection requirements. In particular, the Code requires that the collection and processing of personal information follow the principles of legitimacy, justifiability, necessity and proportionality. The Code also introduces grounds for exemption of liability for those who handle other people's personal information.

© Law Business Research 2021

The PRC Data Security Law, which came into force on 1 September 2021, is a further step in enhancing protection of data security. Among other requirements (such as national security review and requirements on cross-border transfer of important data), the new law requires government approval before companies or individuals can provide data stored within the territory of China to foreign judicial or law enforcement authorities, and further provides that companies providing data to foreign judicial or enforcement authorities without obtaining approval may face fines of up to 5 million yuan, orders to suspend business or revocation of operating permits or business licences.

The PRC Personal Information Protection Law takes effect on 1 November 2021, becoming China's comprehensive law that regulates the collection, processing and transferring of personal information. The Law will also apply to activities conducted overseas that deal with the personal information of individuals who are located in China for certain purposes, such as analysing and evaluating the activities of the individuals to which the personal information belongs. The Law sets out requirements with respect to consent and the lawful basis for dealing with personal information, as well as additional requirements for cross-border transfers of personal data.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The PRC Civil Code protects the privacy rights and personal data of individuals who can bring a civil law claim against the infringer in court. A breach of the CSL may trigger administrative penalties, including a fine, suspension of the business, closure of a website and revocation of an operation permit or business licence. Penalties for violations of the Data Security Law can include an order for rectification, a warning, fines on the entities and their personnel, and, in serious cases, an order for suspension of operations, cessation of business or revocation of operating permits or business licences. A serious violation of core data protection obligation or data export obligation can result in a fine of up to 10 million yuan. Under the Personal Information Protection Law, a company in violation of the rules on the handling of personal information may face a fine of up to 50 million yuan or 5 per cent of the turnover of the previous year, and suspension of business or revocation of operation permits or business licences. An illegal breach of personal data privacy rights could, in serious cases, give rise to criminal prosecution.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Investigations should always be conducted in compliance with applicable data privacy legislation. In recent years, the Chinese authorities have taken an aggressive approach to data privacy violations in the context of internal investigations. For example, as part of an internal investigation, China Auto Logistics collected data about its employees, which the employees subsequently reported to the police. A number of executives of the company resigned following the investigation and the company announced that its securities would be delisted from the NASDAQ stock market in August 2018. Data privacy laws should therefore be borne in mind in the context of investigations and companies should handle relevant data with the utmost care when conducting or responding to an investigation.

© Law Business Research 2021

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Interception of employees' communications by an employer is restricted and must be conducted in accordance with the law.

Interception by employers of employees' communications on employees' personal property is generally prohibited unless explicitly permitted by the employees. It is important for an employer to make clear to employees that they should not have work-related communications on their personal devices, to avoid potential risks of leaks of confidential work-related information.

Interception of employees' communications on employers' devices or systems is possible, subject to compliance with cybersecurity and data protection laws and regulations. Employees need to be made aware that communications on their employer's devices or systems could be intercepted by their employer. This is usually dealt with at the onboarding stage for each new employee. Additionally, prior consent from employees should be obtained for the collection, review, search, holding, processing and transfer of information and communications on the employer's devices or systems for employment-related reasons.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and dawn raids are a common feature of law enforcement in China. Pursuant to the Criminal Procedure Law of the People's Republic of China of 1979 (as amended) (the Criminal Procedure Law), a search warrant issued by a chief prosecutor of a people's procuratorate or the head of a public security bureau (PSB) is normally required before conducting a search in a criminal investigation. However, in emergency situations, including when the person under investigation may conceal, destroy or transfer evidence of a crime, a search may be conducted without a search warrant.

The Supervision Law of 2018 empowers the National Supervision Commission to conduct broad searches and seizure with a warrant. The Criminal Procedural Law authorises investigators from people's procuratorates and PSBs to conduct wide searches and to seize property and documents found during a search to prove a crime. Other authorities (e.g., the State Administration for Market Regulation and antitrust law enforcement authorities) may also conduct searches within the scope of their competence and functions.

Chinese law imposes few limitations on authorities executing search warrants other than the requirement that the search should be witnessed and recorded. Corporations subject to investigation may challenge the authorities' decisions or actions during a search (e.g., restriction of personal freedom, or the sealing up, seizing or freezing of property) before the courts.

© Law Business Research 2021

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privilege in the common law sense is not recognised under Chinese law. Authorities therefore have wide powers to seize documents and, in practice, may demand documents that would be protected from disclosure in other jurisdictions. There is no right to resist the disclosure of legal advice or other categories of evidence.

Although lawyers owe their clients a duty of confidentiality, this does not assist if documents are sought directly from a client or a third party rather than the lawyer. Moreover, under the Lawyer's Law of the People's Republic of China, this duty of confidentiality does not apply to communications aimed at or involving criminal acts causing harm to state security, public security or persons and property. Additionally, this duty may be overridden in the context of investigations. The authorities have a general power to collect or obtain evidence from relevant entities and individuals concerned with a case pursuant to a search warrant or court order.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

There is no right to privilege over documents. Article 52 of the Criminal Procedure Law explicitly prohibits a suspect from being compelled to give evidence to prove his or her own guilt. This protection was introduced in 2012. However, it is ambiguous as Article 52 only limits the measures that interrogators can use to force interviewees to talk. They still have an obligation under the Criminal Procedure Law to answer truthfully all relevant questions put to them. Owing to its imprecise scope and an apparent continued enforcement of the previous law, which afforded no such protection, this right is likely to be of limited use in practice.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Under the Provisions of the People's Procuratorates on Reporting of Crimes 2009 (strengthened in 2014), whistleblowers who report crimes to the enforcement authorities are entitled to protection, anonymity and a right of appeal in the face of refusals to investigate. There is also a reward mechanism for whistleblowers who report crimes to people's procuratorates, and various other financial reward schemes are scattered in sector-specific regulations. The Criminal Procedure Law also contains several measures that protect the personal safety of witnesses giving evidence in legal proceedings and their families, including keeping personal information about witnesses confidential, and adopting protective measures so that the witnesses' appearances or voices are not made public.

An employee who is dismissed for whistleblowing would need to commence an action for wrongful dismissal against the employer, claiming either reinstatement or

© Law Business Research 2021

compensation. Retaliation by employers against whistleblowers in certain circumstances may constitute an offence under the Criminal Law of the People's Republic of China of 1979 (as amended in 1997) and Chinese labour laws. In such cases, the employee should report the matter to the people's procuratorate and the labour authority, as applicable.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Chinese labour laws are generally employee-friendly. In the course of an internal investigation, an employee must continue to be paid in accordance with his or her contract (salary and position are key terms that may only be altered with the mutual consent of the employer and the employee).

During an internal investigation, an employee may submit a dispute to the Labour Dispute Arbitration Commission for resolution. If the employee does not accept the arbitral award, the employee may generally institute court proceedings.

Officers and directors enjoy the same rights as employees. However, an employer may sue officers and directors in a civil action for breach of fiduciary duty separate from an employment claim. Nevertheless, the employer cannot be compensated twice for the same damage.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

If an employee is subject to a criminal investigation by a prosecutor of a people's procuratorate, the employer may suspend the employment contract. If the employee is not convicted of a crime, he or she may ask for state compensation for lost salary and may request reinstatement. If the employee is convicted and sentenced for a crime, the employer may unilaterally terminate the employment on the sentencing date.

In general, as long as an employee continues to be paid his or her basic salary, the company can suspend the employee pending an investigation. As regards dismissal for refusing to participate in an internal investigation, an employee's contract cannot be terminated at will. An employer must have permissible legal grounds, such as a serious violation of company policy by the employee, or if his or her misconduct has caused material damage to the company.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Generally, if an employee refuses to participate in an internal investigation, this is not of itself a sufficient ground for summary dismissal. In practice, terminations are generally agreed privately on the basis of a payment to the employee. Liability for wrongful dismissal is twice the statutory severance.

© Law Business Research 2021

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

This is likely to depend on the nature of the company. Although investigations are not unusual, the management of a Chinese company is unlikely to conduct its investigation in such a structured fashion. Being a domestic company, management and the company's lawyers are also likely to be less concerned about issues such as protecting privilege or procedures for transferring data and state secrets overseas: these matters are likely to be of far less relevance. If, on the other hand, the company is a multinational corporation, the China branch or its lawyers will generally prepare a document setting out the scope of the investigation, which is likely to include such issues.

The scope of any investigation plan will depend on the type and complexity of the issues being investigated, the level of detail needed to brief members of the board or management about the investigation, and the preferences of the company and professionals running the investigation. Generally, it will address who comprises the investigation team, the external lawyers or third-party experts (if any), and the objectives and scope of the investigation. The latter would cover who needs to be interviewed and the document types and date ranges to be searched (addressing privilege and dealing with state secrets and data transfers as appropriate).

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

China's culture is largely a collective, hierarchical one and it is likely that those within the company will report up internally. However, reporting externally is a different matter.

As part of a company's internal investigation, any duty to report the matter to law enforcement authorities or regulators (but see below regarding the case of a regulated entity) should be kept under review.

There is a general duty on individuals and entities under the Criminal Procedure Law of the People's Republic of China of 1979 (as amended) (the Criminal Procedure Law) to report suspected crimes to the public security bureau, the people's procuratorate or the court; however, there is no specific penalty for a failure to do so. Therefore, the provision lacks teeth and the obligation does not tend to be observed in practice, although there have been a number of reported instances of misconduct by employees in the technology sector being reported to Chinese authorities in recent years.

If the company is a regulated entity, for example a financial institution, trading house, insurer or food and drug company, notification requirements are very likely to apply. If it is a domestic, non-regulated entity, it is not common practice that the company will report the issue externally.

In respect of multinational corporations operating in China, there may be more structured processes in place for reporting internally, as well as an awareness and culture of

© Law Business Research 2021

reporting externally. This may also be influenced by the approach of the lawyers representing the entity.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Under Article 54 of the Criminal Procedure Law, an investigating authority may request evidence from relevant entities or individuals. In practice, evidence collection might be accomplished by broad document seizure authorised under a seizure permit. However, it is also possible for an enforcement authority to issue notices for the provision of certain documents or data (especially when the person receiving the notice is not the direct target of the criminal investigation).

There are no strict rules regarding the preservation of documents or electronic data, or the issuing of litigation holds. However, intentional destruction or tampering with evidence is prohibited. Given that a domestic enforcement action could easily attract the attention of enforcement authorities in other countries, it is preferable that a proper litigation hold notification is issued and implemented.

The government is unlikely to allow an entity being investigated to propose its own custodians or search terms. Instead, it might ask the defendant to freeze all electronic data on the system and then conduct its own review of the data collected.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies and unlisted state-owned enterprises (SOEs) are generally not required to make public the existence of an internal investigation or contact from a law enforcement authority.

Under applicable securities laws, issuers and listed companies (including relevant SOEs) must observe their respective information disclosure obligations pursuant to applicable laws. In general, major investigations and litigation must be disclosed in annual and interim reports of listed companies. In addition, listed companies must generally immediately disclose any major event that may have a significant effect on the trading price of its securities.

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal corporate investigations, particularly SOE audits, are common in China. What is quite unusual is self-reporting to local enforcement bodies on the back of an internal investigation. Usually, internal investigations identify remediation steps that are actioned by the company and this concludes the matter. The notion of self-reporting does not generally arise unless it is in the context of foreign enforcement bodies, and parallel reporting to Chinese law enforcement may then be considered.

© Law Business Research 2021

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

No. However, if the conduct in question is, or is likely to be, investigated in a common law jurisdiction, the company and its lawyers should conduct themselves in such a way as to maximise privilege.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

No concept of the attorney–client privilege exists in China. A lawyer owes a duty of confidentiality to his or her client, but this is not akin to legal privilege in the common law sense. In any event, this duty of confidentiality does not apply to communications aimed at or involving criminal acts causing harm to state security, public security or persons and property. This is widely interpreted, rendering the scope of confidentiality protection limited in practice.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Not applicable.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Not applicable.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Not applicable.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

No concept of the limited waiver of privilege exists in China.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Not applicable.

© Law Business Research 2021

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

No concept of common interest privileges exists in China.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Not applicable.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, this is common practice.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

No concept of the attorney–client privilege exists in China.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no strict rules in China relating to the conduct of interviews (such as the requirement to give an *Upjohn* warning). However, the interviewer could be criticised for not explaining the situation or not being transparent (e.g., if the investigation is likely to involve contentious labour law issues). Therefore, from a practical perspective, it is advisable to give something similar to an *Upjohn* warning.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Interviews will usually be conducted at the company's offices, with in-house counsel and external lawyers present. The interview usually involves a chronology covering employment history, the alleged events and the employee's recollections of the events. Assuming they are available, documents will be shown to the employee.

In general, the question of the employee's legal representation will turn on whether the investigation relates to a multinational corporation or a domestic company. A multinational corporation is likely to allow employees to have their own representation, from cultural and risk perspectives (potential exposure in another jurisdiction would militate in favour of allowing separate legal representation for the employee).

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Yes. Under the Criminal Procedure Law of the People's Republic of China of 1979 (as amended), crimes should be reported, but this is not commonly observed in practice. Reporting misconduct to regulators and to law enforcement authorities, as appropriate, is mandatory in most regulated sectors in China.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting in China is often regarded as a confession; indeed, the terms are regularly used interchangeably in a way they are not in the West. The assessment of whether to self-report is generally driven by the risk that a third party may disclose the matter to the authorities. Usually, the risk of an individual disclosing the matter to Chinese law enforcement authorities is lower than in the West.

In practice, and when the matter raises potential liability overseas, a report is usually made to the relevant law enforcement authority in that jurisdiction before anything similar is done in China (e.g., for the purposes of leniency or co-operation credit). Disclosure to foreign law enforcement authorities generally raises the concern that the matter will become public. This in turn may prompt disclosure by the company to the Chinese authorities. Self-reporting is viewed by the Chinese authorities as being highly unusual.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Self-reporting can be challenging in practice. Finding the right person to report to and documenting the report (e.g., for mitigation purposes) is not straightforward. Law enforcement officials may approach the concept of self-reporting with some doubt, and may in turn be reluctant to sign documents or officiate the process. Moreover, it is very unusual in China to involve external lawyers when dealing with regulatory or criminal authorities before charges are laid, partly for reasons of face.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is possible to enter into a dialogue with the investigating authority to clarify the scope of evidence sought, or even to further limit the evidence. This dialogue can be conducted through formal or informal channels, with or without lawyers. However, the investigating authority may choose not to accommodate any such request.

© Law Business Research 2021

55 Are ongoing authority investigations subject to challenge before the courts?

A person or company subject to investigation may bring administrative proceedings against an authority's decision or actions. Pending litigation, the authority's action (e.g., seizing or freezing property) is not usually suspended. In exceptional cases, where non-suspension would result in irretrievable damage or if the relevant administrative authority deems it necessary to suspend the action, the court may, on request, order suspension of the alleged action. The amended Administrative Procedure Law lowered the threshold for bringing an administrative proceeding. However, from a practical perspective, the courts may lack sufficient muscle to deliver judgments without interference from government departments.

Aside from recourse before the courts, an individual may file a petition or complaint to public security bureaux (PSBs) and people's procuratorates against the unlawful exercise of certain powers in an investigation. These do not tend to be reviewed rigorously. In addition, Article 60 of the Supervision Law of 2018 (the Supervision Law) provides for certain acts of the National Supervision Commission (NSC) to be forwarded to a supervisory body for review within a month. It is too early to say whether and how challenges to the NSC's investigative powers will be addressed.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The Chinese authorities are unlikely to limit the scope of their review in consideration of foreign laws. Indeed, since China does not recognise the concept of privilege, the potential scope of disclosure to the Chinese authorities is far broader than under a notice issued by the authorities of common law countries.

The company should seek to comply with each notice, ring-fencing and curtailing disclosure pursuant to applicable laws by asserting legal rights. Issues may arise in China in relation to the transfer of personal data, state secrets and trade secrets overseas. Any appraisal of notices received from another country should ensure that any data and documents are transferred out of the country only in accordance with the limited exceptions provided under Chinese law.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In practice, when a search is conducted and the information sought is located overseas, Chinese authorities have not generally expected companies to search outside mainland China and its Hong Kong and Macao special administrative regions (SARs). The authors are aware of a limited number of circumstances in which material on servers in Singapore has been sought and provided, but this is rare.

Technically, although investigating authorities may seek to impose such a requirement, in general, they may not directly search and seize data overseas. Treaties on mutual

© Law Business Research 2021

legal assistance in criminal matters have been signed by China with 65 jurisdictions as of July 2021 but these are of limited practical assistance in requiring a company to produce documents located overseas. In practice, the investigating authority might use other means (e.g., an administrative penalty) to seek to force a company to comply if the data located overseas is regarded as highly important.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The scope of assistance under bilateral legal assistance agreements includes mutual assistance in taking evidence, executing search and seizure warrants, and producing documents. In this regard, people's procuratorates and PSBs do conduct inquiries into corruption-related matters in response to requests from overseas law enforcement organisations and judicial authorities, or vice versa. Most bilateral agreements on legal assistance contain provisions for tracing, restraining, confiscating, sharing or repatriating the proceeds of crime.

Currently, China's authorities co-operate with SAR enforcement authorities (Hong Kong's Independent Commission Against Corruption and the Macao Public Prosecution Office) in tackling cross-border corruption mainly through a mutual case assistance scheme and practice between the enforcement authorities on the mainland and in the Hong Kong and Macao SARs. In addition, the Supervision Law expressly encourages international co-operation and states that the NSC will coordinate anti-corruption co-operation with relevant countries, regions and international organisations, and implement anti-corruption international treaties.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

People's procuratorates or PSB investigators must keep the following information confidential: the identity of the person who makes the complaint; the identity of any suspects; the identity of any witnesses; and any state secrets, trade secrets and matters of personal privacy or personal information. These provisions are intended to contain dissemination of information to third parties. The Supervision Law expressly requires the NSC to keep state secrets, trade secrets and personal privacy confidential. Given the NSC's power to involve other authorities in its investigations, sharing other information with third parties should be expected.

In general terms, an investigation should be kept confidential. By disclosing matters about an investigation to a third party, a person may fall foul of Article 50 of the Law on Penalties for Administration of Public Security. Article 50 punishes those who obstruct a functionary of a state organ (which includes the various investigating bodies) from performing their duties.

© Law Business Research 2021

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

It is not typical for Chinese law enforcement authorities to request documents located overseas from a Chinese company. If they do, and to comply would violate the laws of the other country, this should be explained. The Chinese authorities will generally respect this. Though this should not be necessary, the company could seek a legal opinion setting out how disclosure would violate those laws.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

At the end of 2018, China enacted the International Criminal Judicial Assistance Law, which governs how assistance is provided to foreign authorities and other bodies in criminal investigations. This Law may serve as a blocking statute and restrict cross-border discovery of evidence. Institutions, organisations and individuals within China may not provide assistance to foreign countries without the consent of a competent authority, which may refuse on several grounds. In addition, the Cybersecurity Law (CSL), the Data Security Law and the Personal Information Protection Law attempt to harmonise rules on cross-border transfers of personal data. Draft regulations issued under the CSL indicate that personal and other important data can be transferred offshore only subject to a security assessment by the government authority.

A related point concerns state secrets in the context of foreign notices or subpoenas. State secrets are defined very broadly. Therefore, the content of documents may be classified as a state secret under Chinese national security legislation. There is a risk that an investigation of Chinese documents may implicate state secrecy matters. This will also affect the ability to transfer documents overseas in response to a notice or subpoena.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Disclosure to the Chinese authorities is generally compelled in an investigation. Although a producing party can assert that confidentiality attaches to the investigation conducted by the Chinese authority, whether that assertion will create an effective shield from disclosure will depend on the relevant Chinese and foreign laws. For example, pursuant to Chinese law, documents containing state secrets should not be disclosed to a third party.

Confidentiality requirements in China are very general and are unlikely to prevent the sharing of documents provided that disclosure is within the purview of Chinese law. Once documents have been shared with law enforcement authorities, a company cannot guarantee that they will not be shared with third parties. It is important for the company to assert its legal rights pursuant to the laws of the relevant jurisdictions so as to limit contagion issues.

© Law Business Research 2021

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

A corporate entity found guilty of misconduct will generally be sanctioned by a fine. The personnel in charge of the company and other personnel responsible for the crime may also face criminal liability (imprisonment, fines and confiscation of assets). In addition, individuals who have been convicted of corruption or bribery offences may also be disqualified from being directors or in senior management for five years. Further, an individual who has committed crimes by taking advantage of his or her profession or violating his or her duties may be prohibited from engaging in relevant professions for between three and five years.

As regards bribery offences, the April 2016 Judicial Interpretation to the Criminal Law of the People's Republic of China of 1979 (as amended in 1997) (the Criminal Law) introduced monetary thresholds for sentencing linked to the severity of the offence. For those in the private sector, individuals can be sentenced to up to 10 years' imprisonment for an offence of giving or offering a bribe and (technically) up to 15 years for receiving a bribe. Corporates committing bribery offences are liable on conviction to fines ranging from 100,000 yuan to twice the amount of the bribe.

For civil bribery offences under the Anti-Unfair Competition Law, a corporate entity may face administrative fines of up to 3 million yuan, revocation of business licences and confiscation of illegal gains.

The Supervision Law of 2018 (the Supervision Law) expressly empowers the National Supervision Commission to confiscate, recover or order restitution of ill-gotten gains. It should transfer those assets to the people's procuratorate to then prosecute in the usual way.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Government procurement is conducted by local government under the general guidelines set out in the Government Procurement Law. Serious illegal conduct (i.e., any conduct that results in criminal liability, revocation of business licence or large civil fines) within the previous three years should disqualify an entity from participating in government procurement under Article 22 of the Government Procurement Law. In addition, misconduct during government procurement (e.g., corrupt acts that result in a fine ranging from 0.5 per cent to 1 per cent of the procurement value) will also disqualify an entity from participating in future government procurement for between one and three years under Article 77 of the Government Procurement Law. Although there is no national registry of qualified government contractors, the government has maintained a publicly available list of suppliers subject to debarment under Article 77 of the Government Procurement Law, and information regarding serious illegal conduct under Article 22 is generally accessible via company searches on the websites of relevant Chinese authorities.

© Law Business Research 2021

65 What do the authorities in your country take into account when fixing penalties?

Under the Criminal Law, the Chinese courts should take into account factors including the nature of the crime, circumstances relating to the criminal conduct and the damage caused to society. Circumstances relating to the criminal conduct include aggregating or mitigating factors, such as whether it is a first or repeat offence, or self-reporting. Additionally, the courts may exercise discretion in considering other circumstances, such as motive, the surrounding circumstances and whether there was any confession.

Regarding criminal bribery offences, both the ninth amendment to the Criminal Law (November 2015) and the April 2016 Judicial Interpretation provide clarification on the effects of self-reporting and co-operation. Generally, if the crimes are relatively minor or the offender has 'played a key role in investigating or solving a major case', self-reporting may mitigate or even exempt the offender from liability. Otherwise, offenders who self-report should be entitled to lenient treatment, but cannot expect to be exempted from liability. The Supervision Law also proposes leniency when a person surrenders or voluntarily confesses, actively co-operates with the authorities, takes active measures to disgorge ill-gotten gains or otherwise renders significant assistance in cases involving major national interests.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No such settlement scheme exists in China.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No such settlement scheme exists in China.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

No such settlement scheme exists in China.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Historically, it was not typical for Chinese law enforcement authorities to use external corporate compliance monitors as an enforcement tool. However, since the Supreme People's Procuratorate's launch of the pilot programme of 'Corporate compliance non-prosecution reform' in March 2020, the Supreme People's Procuratorate has issued a few model cases in which local people's procuratorates entered into compliance monitor

© Law Business Research 2021

agreements or used corporate compliance monitors. Further to the expanded scope of the programme into more local people's procuratorates in more provinces and the introduction of the guidance on compliance monitoring this year, we anticipate seeing more cases that would involve external corporate compliance monitors as an enforcement tool going forward.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes. However, this is rarely encountered given the domestic litigation environment, and the documents and files of the authorities would not be made available for a civil action. Also, authorities cannot share information classified as a state secret under the Chinese national security legislation.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

At the investigatory stage, a confidentiality requirement is imposed through a general provision in the Criminal Procedure Law of the People's Republic of China of 1979 (as amended). By disclosing confidential matters about an investigation, a person may fall foul of Article 50 of the Law on Penalties for Administration of Public Security.

Once a case is before a court, the trial should technically be conducted with full public access unless state secrets, trade secrets or issues attracting privacy rights are implicated. Judges often take a very conservative approach, and access to the court by journalists and the general public is limited in practice. Although there is no general restriction on publicising a case during the trial process, this is rare in practice and parties to litigation are generally advised not to make public statements during trials.

Chinese media outlets are controlled by the state, for the most part. As such, investigations and trials involving state-owned enterprises (SOEs), or broader public industry issues, are not fully reported in China (in contrast to overseas or Hong Kong media). On the other hand, the major private sector criminal investigation into GlaxoSmithKline was reported in both China and overseas.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

The way in which corporate communications are managed will depend on the nature of the company (whether an SOE, a privately owned Chinese company, a listed company or a multinational corporation with operations in China). For the most part, it would be unusual for a public relations firm to be retained. However, this has occasionally been seen in high-profile matters involving multinational corporations or large multi-jurisdictional investigations involving the US authorities.

© Law Business Research 2021

73 How is publicity managed when there are ongoing related proceedings?

Related proceedings may be in the public domain and, therefore, could attract more publicity. Generally, statements to the press about current litigation should be limited, and contagion issues should be managed carefully throughout. Leaks to the press are not advisable; the parties should focus on the issues within the public court arena.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

There is generally no such mandatory disclosure requirement under corporate laws.

Under the PRC Security Law and related regulations, publicly listed companies are required to issue a market announcement of any major events that may materially affect the trading price of their shares. Although not specifically stated, settlement of criminal proceedings could constitute a major event, provided it materially affects the share price.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

ESG matters are regulated by various Chinese administrative authorities at national, provincial and municipal levels. In the environmental field in particular, China has one of the most comprehensive frameworks of environmental protection laws. Key statutes include the Environmental Protection Law, the Environmental Impact Assessment Law and the Energy Conservation Law. The main government authority responsible for regulation and enforcement of environmental matters is the Ministry of Ecology and Environment (formerly the Ministry of Environmental Protection and, prior to 2018, the State Environmental Protection Administration).

In terms of recent developments, on 28 June 2021, the China Securities Regulatory Commission published updated disclosure rules relating to annual reports and half-yearly reports for listed companies. The revised rules, which came into effect on the same date, set out a number of mandatory and voluntary ESG disclosure requirements. According to the rules, 'key polluting entities' (as defined by environmental authorities) are required to disclose certain information in their annual reports, including detailed pollutant discharge information, details of pollution prevention and control facilities, an environmental impact assessment of planned and current projects, environmental emergency response plans and self-monitoring plans. The revised rules also require all listed companies to disclose any administrative penalties incurred during the reporting period arising from environmental issues.

Additionally, the rules contain a number of items, the disclosure of which is encouraged for all listed companies but not mandated, including information about measures taken to reduce carbon emissions, and information relating to the fulfilment of social responsibilities (including, for example, the protection of rights and interests of shareholders, creditors, employees, suppliers and customers, and efforts to support poverty alleviation in rural areas).

© Law Business Research 2021

On 16 July 2021, China opened its long-anticipated national carbon emissions trading scheme. It is the largest of its kind in the world, covering more than 2,000 entities with aggregate annual emissions exceeding four billion tons of carbon dioxide equivalent.

This 'cap and trade' scheme incentivises cost-effective reductions in emissions and generates a price on emissions to be paid by the heavy emitters. Entities covered by the scheme must follow an annual compliance procedure of monitoring, reporting and verification. A covered entity falsely reporting or concealing its emissions data, or refusing to report its emissions, can be subject to fines of between 10,000 and 30,000 yuan, while a covered entity that does not duly fulfil its obligation to surrender sufficient carbon allowances within the mandated deadline can be subject to fines of between 20,000 and 30,000 yuan.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Although we are not aware currently of any specific developments on the horizon, ESG matters (particularly environmental concerns) are a significant area of focus for Chinese authorities and we expect to see further developments in this area in the coming years. Businesses operating or investing in China should ensure they stay abreast of the latest regulations in order to remain compliant.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

We are not aware of any private actions being brought in respect of ESG issues in China. The legal and political landscape in the country means that the type of litigation typically initiated in other jurisdictions by non-governmental organisations is unlikely to occur in China. We have witnessed an increase in enforcement initiatives targeting specific industries, including thermal power, mining, steelmaking and construction, and we would expect this trend to continue in line with the government's continuing focus on environmental issues.

Following recent revisions to disclosure rules for listed companies, it remains to be seen whether this will lead to an increase in enforcement action, in response either to disclosure of non-compliant actions or to suspected false or incomplete disclosures.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

There have been a number of changes that are designed to address both corporate and public misconduct. These include amendments to the Anti-Unfair Competition Law (AUCL) and the introduction of both the Supervision Law of 2018 and the International Criminal Judicial Assistance Law. There have also been administrative and structural changes to the enforcement of key legislation in this area, including the introduction of the National Supervision Commission and the State Administration for Market Regulation (SAMR). The SAMR administers the AUCL and other antitrust legislation.

© Law Business Research 2021

We anticipate that the regulators and authorities will continue to focus on enforcement under these new laws, rather than further amendments. In fact, we have already seen a significant number of investigations commenced by these bodies.

With the introduction of the Data Security Law, the Personal Information Protection Law, the Export Control Law and the Anti-Foreign Sanctions Law, we anticipate a shift by regulators towards issuing more detailed guidance and enforcement.

That said, the recent focus on investigations in specific sectors may result in changes to the regulations or the publication of additional guidance to allow authorities to more closely monitor and regulate activities in the pharmaceutical and technology sectors.

© Law Business Research 2021

10

Colombia

Pamela Alarcón Arias[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigations in Colombia are those regarding corruption in public contracts, and concessions in sectors such as infrastructure, health and public functions.

Criminal and administrative investigations that gain the highest profile are those that relate to illegal awards of public contracts, collusion and bribery to obtain public contracts and concessions, and breach of contract to the detriment of public finances and goods.

Odebrecht is currently the highest-profile investigation in Colombia, because of the amounts of money involved; the company has acknowledged paying US$11 million in bribes to government officials between 2009 and 2014 and US$6.5 million in relation to the contract for the Ruta del Sol 2 toll road concession.

As part of the criminal investigations, several other people, including a vice minister, a senator and the former president of Corficolombiana, have been sentenced for their involvement in the *Odebrecht* corruption case.

2 Outline the legal framework for corporate liability in your country.

One of the principles of Colombia's criminal law is *societas delinquere non potest*, whereby corporations cannot be held criminally liable. Nevertheless, it is possible for a corporation to be civilly liable in a criminal matter when the conduct of its employees or directors is related to their work or activities within the corporation, such as corruption (Colombian

1 Pamela Alarcón Arias is a partner at Philippi Prietocarrizosa Ferrero Du & Uría.

© Law Business Research 2021

Criminal Procedure Code and Law 600, 2000). The Attorney General's Office enforces the sanctions and judges rule on the cases.

In terms of administrative liability concerning corrupt conduct, two principal authorities oversee the imposition of sanctions on corporations:

- The Superintendence of Companies imposes administrative sanctions on companies for conduct involving transnational corruption, under Law 1778, 2016. Additionally, when a sentence is executed against a legal representative or an administrator of a company located in Colombia or a branch of a foreign company, the Superintendence of Companies could impose a fine on the corporation of up to 200,000 times the minimum monthly wage.
- Antitrust practices such as collusion could also be liable to administrative sanctions on corporations as enforced by the Superintendence of Industry and Commerce (Law 155, 1959; Law 256, 1996; Decree 2153, 1992; Law 1340, 2009).

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Administrative sanctions relating to transnational bribery are enforced by the Superintendence of Companies under Law 1778, 2016.

Other administrative sanctions linked with corrupt practices against free competition are enforced by the Superintendence of Industry and Commerce (Law 256, 1996; Decree 2153, 1992; Law 1340, 2009).

Civil sanctions relating to criminal activities are enforced by the Attorney General's Office, under the Criminal Procedure Code and Law 600, 2000.

Jurisdiction is allocated between the authorities depending on whether the case is civil, administrative or criminal. However, different authorities can pursue a corporation at the same time for the same conduct if there have been infringements of different laws or regulations.

Authorities may have internal policies or protocols relating to the prosecution of corporations; nevertheless, procedures are established in laws, decrees and circulars.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The Attorney General's Office is obliged by law to initiate an investigation following a criminal complaint or receipt of information relating to a criminal complaint. There is no need to corroborate the information before the initiation of an investigation. However, prosecutors have the duty to verify the information and gather new evidence before the indictment.

In the same way, administrative authorities, such as superintendencies, have a broad discretion to initiate investigations.

© Law Business Research 2021

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Under Colombia's legal framework, natural and legal persons are encouraged to co-operate with the authorities. However, the lawfulness of a notice or subpoena may be challenged in any case with a constitutional action, such as a writ for protection of fundamental rights (*amparo*).

Depending on the law enforcement authority and the jurisdiction, and when the procedures allow, ancillary claims or appeals against a subpoena or notice can be made before a fundamental guarantees judge.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Depending on the jurisdiction, co-operative agreements can be made with different authorities.

For some criminal matters, prosecutors may apply the principle of discretionary prosecution (Criminal Code, Article 324) or reach a settlement with natural persons who assist or co-operate with authorities.

Under Decree 1523, 2015, companies and natural persons involved in a business cartel may denounce its existence, acknowledge their participation and provide evidence that will allow the authorities to sanction the other participants, and thus obtain total or partial leniency of any fine imposed by the Superintendence of Industry and Commerce for an infringement of free competition.

Additionally, Article 7 of Law 1778, 2016 establishes that sanctions for transnational bribery could be adjusted in consideration of criteria such as collaboration, acknowledgement or express acceptance of an offence. Nevertheless, the sanction adjustment would not apply for repeated conduct.

7 What are the top priorities for your country's law enforcement authorities?

The top priorities for Colombia's law enforcement authorities are currently illegal drug trafficking, money laundering, financing of terrorism, corruption, collusion in bidding and tendering processes, and antitrust practices.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

An effective compliance programme depends on the economic sector in which a company operates, on its risk assessment, adequacy of resources and tone from the top, among other things.

© Law Business Research 2021

Nevertheless, Colombian regulation states that an effective compliance programme (e.g., for the real sector, which comprises industrial and utilities services) shall include prevention measures for money laundering, the financing of terrorism, financing the proliferation of weapons of mass destruction, acts of foreign bribery and corruption and other provisions described in the External Circulars of the Superintendence of Companies No. 100-000016, 2020, Chapter X and No. 100-000011, 2021.

A compliance programme that has been enforced effectively could enable a reduction in administrative sanctions and criminal penalties imposed on a company following the commission of bribery or transactions that involve illegal assets, and for which the company could be held liable.

Other relevant Colombian laws and guidance are the Transport Superintendence, Law 1762, 2015; the Colombian tax authority's External Circular 170, 2002; and the Superintendence of Finance, External Basic Circular 029, 2014, Chapter IV, Title IV, Part I.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Guidance on cybersecurity is established by the National Council of Economic and Social Policy (CONPES). Three strategy documents – CONPES 3701, 2011; 3854, 2016; and 3995, 2020 – set forth national cybersecurity policy guidelines with the aim of developing a national strategy to counteract the increase in computer threats that significantly affect the country. In this frame of reference, 'cybersecurity' is defined as the capacity of the state to minimise the level of risk to its citizens and the degree to which they may be affected by cybernetic threats or incidents.

There is a broad national legal framework for cybersecurity relating to data protection, cybercrime and e-commerce, among other things.

There are separate guidelines for corporations regarding cybersecurity. For example, the Ministry of Information and Communications Technology (MINTIC) – which is in charge of promoting the access, effective use and mass appropriation of information and communications technology – has issued guidance regarding the security and privacy of information, and for the assessment of digital security risk assessment, namely MINTIC, Cloud safety, security and privacy of information; MINTIC, Security Model and Information Privacy; and MINTIC, Strategic Innovation Agenda: Cybersecurity.

Finally, enforcement action in relation to companies' preparedness for and response to data breaches is taken by the Superintendence of Industry and Commerce. The majority of such incidents concern data breach protection. However, when breaches become felonies, criminal investigations may be initiated by the Attorney General's Office.

© Law Business Research 2021

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Through Law 1273, 2009, Colombia has included in the Criminal Code more than 10 crimes relating to cybercrime. Under Law 1928, 2018, Colombia adopted the Budapest Convention on Cybercrime.

Special units have been created within the national police service and in the Attorney General's Office to enforce cybercrime prevention and investigations.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Colombian criminal law has extraterritorial effect in six situations, as set out in Article 16 of the Colombian Criminal Code:

- if a person carries out any of the following acts in a foreign country:
  - crimes against the security of the Colombian state;
  - crimes against the constitutional system;
  - crimes against economic policy (excluding money laundering crimes);
  - crimes against public administration;
  - counterfeiting Colombian currency; or
  - financing terrorism;
- if a person working for the Colombian state is covered by international law immunity and perpetrates a crime in a foreign state;
- when a person working for the Colombian government is not covered by international law immunity but commits a crime other than those listed above, provided the perpetrator has not been convicted of that crime in the foreign country;
- if a Colombian person, except in relation to the aforementioned felonies, is in Colombian territory after committing a crime abroad, and when the sanction under Colombian criminal law is imprisonment for no less than two years, provided the perpetrator has not been convicted of that crime in the foreign country;
- if a foreigner (other than a person described above) is in a Colombian territory after committing a crime abroad that affects the Colombian state or a Colombian national, and when the sanction under Colombian criminal law is imprisonment for no less than two years, provided the perpetrator has not been convicted of the crime abroad; or
- if a foreign person perpetrates a crime abroad against another foreigner. Nevertheless, the crime must comply with the following conditions:
  - the offender must be in a Colombian territory;
  - Colombian criminal law sanctions the crime with imprisonment for no less than three years;
  - the crime is not political; and
  - extradition has not been granted.

© Law Business Research 2021

Besides the aforementioned legislation, Colombian criminal law has extraterritorial effect for prosecuting cross-border bribery of a foreign public official in international transactions. This is regulated in Article 433 of the Colombian Criminal Code. (Note that Colombian criminal law only pursues individuals, not corporations.)

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges that arise in cross-border investigations in Colombia are:

- to accomplish constant and effective communication between the two countries' authorities that are in charge of the legal investigation and prosecution of the crimes;
- to ensure that each country's authorities fully exchange useful information pertaining to criminal investigations;
- to ensure effective co-operation between the countries involved so as to carry out the legal investigation and prosecution of the felonies;
- in the event that the countries have different laws regarding the same event, to identify which legal framework is applicable; and
- to ensure that the legal authorities in the countries involved in cross-border investigations (1) apply any precautionary measures requested by other states and (2) pursue assets relating to foreign felonies requested by other states.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy is established in Article 8 of the Colombian Criminal Code, specified as a prohibition of double criminality, in that no person can be charged more than once for the same criminal conduct, regardless of the name given to the conduct in other countries (provided that the core set of facts are the same).

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not legally binding nor are they common. However, Colombia has signed international treaties and co-operation agreements with various countries, including Peru, Brazil and Spain, for mutual assistance in pursuing certain crimes, such as cross-border bribery and corruption.

© Law Business Research 2021

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

According to the Colombian legal system in criminal matters, the decisions issued by a foreign authority abroad shall be legally binding for all judicial proposes. Therefore, the notion of prohibition of double criminality or double jeopardy would also apply in this case.

However, this rule does not apply to decisions made abroad in connection with the following situations:

- when a Colombian national commits a crime abroad on a state-owned or state-operated ship or aircraft;
- when a person commits any of the following felonies in a foreign country:
  - crimes against the security of the Colombian state;
  - crimes against the constitutional system;
  - crimes against the economic policy (excluding money laundering);
  - crimes against public administration; or
  - counterfeiting Colombian currency; or
- if a person working for the Colombian state, who is covered by international law immunity, perpetrates the crime abroad.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

In an administrative case that falls under its jurisdiction, the Superintendence of Companies can impose the following administrative sanctions on a corporation for conduct constituting transnational corruption (Law 1778, 2016): (1) disqualification from contracting with the Colombian government for up to 20 years; (2) a fine of up to 200,000 times the statutory monthly minimum wage; (3) publication in national newspapers, and on the website of the sanctioned legal entity, of an excerpt from the sanctioning administrative decision, for up to one year; or (4) disqualification from receiving any type of incentive or subsidy from the government for five years.

Since Colombia does not have criminal liability for corporations, the sanctions on natural persons in a case of bribery could be imprisonment, a fine of between 66.66 and 150 times the statutory monthly minimum wage, or disqualification from contracting with the Colombian government for up to 20 years.

However, according to Law 1474, 2011, the disqualification from contracting with the Colombian government will extend to the corporation, its parent, its subordinates and the branches of foreign companies, with the exception of limited companies, if (1) the actions of the natural person involved in corruption crimes relate to the corporation's activities and (2) if a convicted person is an administrator, legal representative, member of the board of directors, or controlling partner or shareholder of the company.

Currently, numerous corruption investigations are being carrying out by different authorities; nevertheless, to date, only the Superintendence of Companies has imposed

© Law Business Research 2021

a significant fine on a corporation (of 4.6 billion Colombian pesos) in the framework of an agreement.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Since Law 1778, 2016 came into force, there has been an increase in enforcement activity relating to corruption investigations involving corporations and individuals; nonetheless, most of them are still under investigation, and therefore no sanctions have yet been applied.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Law 1573, 2012, promotes co-operation between the Colombian authorities and their counterparts in other countries for the purposes of enforcement of anti-corruption legislation. The Criminal Procedure Code and statutes such as Law 1778, 2016, also allow for international co-operation in investigations.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Colombia has not enacted any blocking legislation in relation to the sanctions measures of third countries. However, Colombia is a party to the United Nations Security Council Consolidated List of sanctions and it is common practice for reference to be made to the sanctions list compiled by the Office of Foreign Assets Control of the US Department of the Treasury.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct in Colombia most often come to light by means of media reports and criminal complaints. It has become more common that former employees file complaints against companies they have worked for; therefore, whistleblowers are also relevant in allegations of misconduct. Note that collaboration agreements for whistleblowers continue to be vigorously enforced by the authorities.

© Law Business Research 2021

INFORMATION GATHERING

22 Does your country have a data protection regime?

Individuals in Colombia have the constitutional right to be aware of, update and rectify the information about them held on databases. This constitutional right is implemented by specific legislation on personal data protection and privacy: primarily by Law 1581, 2012; Law 1712, 2014; Decree 1377, 2013; Decree 1074, 2015; and certain additional implementing regulations.

There is also a separate specific regulation, primarily contained in Law 1266, 2008, that regulates the collection, use and transfer of financial information (i.e., credit, risk and banking information).

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The data protection regime is enforced by the Superintendence of Industry and Trade (SIC), which has the power to initiate administrative investigations, *ex officio* or at the request of an interested third party. The SIC is active in its enforcement of the data protection regime, but the likelihood of an enforcement action will ultimately depend on the type of irregularity or infraction, and how it is brought to the SIC's attention. For any kind of violation of Colombian data protection regulations, the SIC may:

- impose sanctions (e.g., fines of up to 1.475 billion pesos, temporary suspension or cancellation of activities relating to data processing); or
- order preventive measures (e.g., issue instructions to protect personal data).

The SIC may also co-operate with international data protection authorities when a foreign legal entity is violating the data protection rights of individuals located in Colombia.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Under Colombian data protection regulations, any type of processing of personal data requires prior and informed consent. Moreover, personal data must be collected for specified, explicit and legitimate purposes. Thus, save for certain exceptions (e.g., public data, or information required by a government entity or in connection with judicial proceedings, among other things), personal data may only be processed with prior consent and for the specific purposes for which it was collected.

Additionally, even in an internal investigation, individuals must be afforded all the rights granted by data protection laws.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The interception of employees' communications may be legal as part of an internal audit or investigation. Nevertheless, the scope of that interception must remain restricted to

© Law Business Research 2021

corporate emails and other correspondence relating to company matters. Investigation of any other communications will be illegal without prior authorisation by a judge.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes. According to Articles 219 to 232 and 237 of the Criminal Procedure Code (Law 906, 2004), the following legal limitations apply to any authority executing a search warrant or a dawn raid:

- a written order from the prosecutor must exist, unless:
  - the owner or the holder of the property agrees with the authorities that the written order is not necessary;
  - the property is an open field, abandoned or in full public view; or
  - there is an emergency;
- a written order must be limited to a specific area of the property;
- the purpose of the written order is to gather evidence or to capture the possible liable person;
- a probable cause shall exist concerning the existence of evidence or that the possible liable person is inside the property; and
- a judge must study the dawn raid procedure within 24 hours of the competent authority submitting its activity report and confirm whether Colombian law has been respected.

If the above conditions are not met, the authority cannot admit any of the evidence that has been collected, and if a person has been captured, the authority must free him or her.

Furthermore, although there is no automatic redress, if the limitations are not observed, there may be legal consequences for the authority, such as for prevarication.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

During a dawn raid, a company or natural person can ask the authority in charge directly not to seize privileged material. If the authority nevertheless seizes this kind of material, the company or natural person can note this irregular situation in the dawn raids record.

Furthermore, the company or natural person whose privileged material has been seized can ask for a hearing to be held, at which a judge will study the specifics of the case and determine whether the material should have been seized.

The authority must exclude from the investigation and process all privileged material that could be seized unlawfully.

© Law Business Research 2021

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The general rule for an individual's testimony to be compelled is that anyone with knowledge about relevant facts that are investigated by the authority has the duty to testify. The person testifying must refer only to the truth, or otherwise be at risk of committing perjury. The principal exceptions to this duty are the privilege of professional secrecy and the right against self-incrimination or incriminating a relative.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

In view of Colombia's history of civil war and the fight against illegal drugs and terrorism, there is a broad protection programme for informers, victims and public officials, mostly in connection with investigations relating to terrorism, illegal drugs, sexual harassment and violence. Nevertheless, in high-profile corruption cases too, whistleblowers may request protection.

The programme is under control of the Attorney General's Office and the National Protection Unit. There are also financial incentive schemes for whistleblowers, which are authorised by the government through the Ministry of Defence.

Further, Article 19 of Law 1778, 2016, and Article 14 of Decree 2896, 2010, establish some benefits for whistleblowers in transnational corruption cases and for antitrust practices, such as total or partial exoneration of an administrative sanction.

The Superintendence of Companies also promotes the existence of whistleblower channels in corporations as good anti-corruption practice.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Colombian law does not limit employees' rights within the scope of internal or external investigations and there is no distinction between officers or directors for these purposes. Nonetheless, employees whose work requires monitoring and enforcing could be subject to internal company controls or have their employment agreement terminated if they are found to be in breach of their labour obligations.

To sanction an employee, a company must comply with the disciplinary procedure incorporated in both its employee handbook and the constitutional guidelines set forth in Ruling C-593 of 2014, which require the employer to notify the employee of:

- the date of the disciplinary procedure;
- the possibility of being accompanied by a co-worker during the procedure; and
- the misconduct that led to the procedure.

© Law Business Research 2021

In addition, the employee has the right to:
- provide evidence and arguments that contradict the allegations made by the employer;
- evaluate the evidence submitted by the employer; and
- appeal any and all sanctions imposed.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Colombian law does not limit or differentiate rights for employees who are considered to have engaged in misconduct. A company may take disciplinary measures against those employees, following the disciplinary procedure set forth in its employee handbook and the constitutional guidelines.

Furthermore, employees whose job descriptions include additional ethical compliance obligations may have their employment agreement terminated for cause, in which case they shall not be entitled to the legal severance payment.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Yes. If this conduct has been included in the employment contract, handbook or company policy as a cause for termination of an employment agreement, the employer may terminate the labour relationship with cause.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Preparing a document setting out the terms of reference or investigatory scope before commencing an internal investigation will depend on a company's internal audit structure, its experience and the information available. However, it is common for internal auditors and members of a company's compliance department to do this.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are no internal steps that companies are legally required to take. Nevertheless, it is important for the company to follow its own good practice policy. For instance, first, the company should conduct an internal investigation (using internal resources or hiring a third party who is a specialist in auditing and risk consultancy) to enable it to gather information and documentation about the issue. Once the issue has been analysed and the

© Law Business Research 2021

compliance officer has assessed the risk, it is important to report the matter to the board. The compliance officer may consult an expert to gain an understanding of the possible consequences for the company, and thus be able to offer proper advice to the board regarding the best course of action to be taken. The board will decide whether to denounce the issue to the authorities, provided it is not mandatory under the Criminal Code.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Colombia's legal framework encourages individuals and corporations to co-operate with the authorities. Nevertheless, the lawfulness of a notice or subpoena may be challenged in any case with a constitutional action, such as a writ for the protection of fundamental rights (*amparo*) or, in a criminal case, before a fundamental guarantee judge.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Both an internal investigation and contact from a law enforcement authority are confidential; therefore, there is no legal obligation to publicly disclose their existence.

Decree 2555, 2010 establishes that companies registered on the Colombian Stock Exchange must disclose 'relevant events'. Contact from a law enforcement authority could be interpreted as a relevant event if, for example, it could affect the share price or the value of the company.

37 How are internal investigations viewed by local enforcement bodies in your country?

The authorities always welcome internal investigations as a sign of co-operation. There are no requirements regarding the conduct or form of internal investigations, except for labour internal investigations, which must follow the disciplinary procedure incorporated in both a company's employee handbook and the constitutional guidelines set forth in Ruling C-593 of 2014.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Attorney–client privilege may be claimed over communications or any kind of information exchanged between a lawyer and a client.

A company should have a professional relationship (i.e., a written contract) with external counsel and all communications or information shall refer to the matter of

© Law Business Research 2021

this relationship. Furthermore, the protected material shall specify that it is covered by attorney–client privilege.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There is a general obligation for all professionals, including attorneys, to maintain professional secrecy. Article 74 of the Colombian Constitution sets forth that professional secrecy is inviolable. This privilege protects privacy as its underlying interest (Article 15, Colombian Constitution).

Attorneys must refuse to disclose or testify about a client's information. Lawyers cannot be compelled to testify against their clients. Nevertheless, lawyers can be excused from complying with this duty if they know that a crime has been, or is going to be, committed.

The holder of the attorney–client privilege is the client.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Although there is not a specific law that differentiates between in-house and external counsel regarding professional secrecy, currently it is considered that the privilege applies only to external counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The attorney–client privilege applies equally to advice sought from foreign lawyers in relation to an investigation in Colombia.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The waiver of the attorney–client privilege is not necessarily considered a co-operative step. What triggers co-operative conduct is the fact that any person will share information about the investigation. In addition, there is not a specific context in which the privilege waiver is mandatory. However, a lawyer will not be penalised if he or she contributes to stopping a crime from being committed.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. As the client is the holder of the privilege, he or she can specify which part of the information he or she wishes to share and with which authority.

© Law Business Research 2021

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If privilege has been waived on a limited basis in another country, it can be maintained in Colombia.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privileges does not exist in Colombia.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes. This could pertain to a new relationship protected with a new privilege, or part of the attorney–client privilege if the assistance is in respect of the same matter.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Colombia allows witnesses to be interviewed as part of an internal investigation.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

The attorney–client privilege includes all the activities and information known by the attorney if they relate to the attorney–client relationship. A company can claim the attorney–client privilege in this situation.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

When interviewing an employee or a third party in Colombia, the following steps are recommended:

- informing the interviewee:
  - who is the attorney's client;
  - that he or she has the right to have his or her own representation;
  - about the facts that are being investigated and the purpose of the interview;
  - that only the truth is expected and that possible falsehoods will be communicated to the authority; and
  - (if he or she is an employee) about the company's relevant internal policies;
- avoiding incriminating questions; and
- drawing up a record of the interview, which should include a signed declaration by the witness that the deposition was given voluntarily.

© Law Business Research 2021

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

An internal interview will typically include the following:

- an explanation of the nature of the investigation;
- asking questions to elicit personal information about the interviewee and his or her background;
- asking the witness about the facts being investigated;
- putting to the witness relevant documents found during the investigation – with prior authorisation from the client – and asking him or her about them; and
- listening to the witness's deposition.

The interview should be recorded and that record should be signed by the interviewee.

Employees may have their own legal representation at the interview.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Article 67 of the Criminal Procedure Code sets forth a general duty of reporting misconduct to law enforcement authorities. Nevertheless, in accordance with Article 441 of the Criminal Code, a penalty for non-compliance with this obligation will only be applicable when the misconduct relates to genocide, enforced displacement, torture, enforced disappearance, homicide, kidnapping, terrorism, illicit enrichment, drug trafficking, money laundering or any other misconduct that may affect sexual integrity.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

A company should self-report to law enforcement when any misconduct has been committed that jeopardises the company's legal activity, even if there is no legal obligation to do so.

In addition, the company should self-report in other countries when the misconduct could have a negative effect outside Colombia.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

An internal investigation regarding the misconduct should be carried out, and all relevant documents and information collected. The company should be advised about the legal consequences of the misconduct and the self-reporting. Depending on the case, the company should hire an attorney to ascertain the legal requirements for the self-report and its consequences.

© Law Business Research 2021

The person or entity should co-operate with the competent authority during the investigation and ask the authorities to be admitted as a victim, provided this possibility is pertinent to the case.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Prior to filing charges, it is customary that the authorities enter into a dialogue with the company (except in a criminal investigation). The company should appear before the authority within the established notification period, be engaged in the case so that it can be informed, provide the necessary evidence and exercise its right to a defence.

The Colombian administrative sanctioning proceeding involves a preliminary investigation in which the authority determines whether there are reasons to open a formal investigation and to file charges. During the preliminary investigation, the authority is allowed to request the company's information, make inspections of the company's facilities, examine computers and obtain testimonies from the company's workers, officers and directors.

Throughout a preliminary investigation, some authorities, such as the Superintendence of Industry and Commerce, may allow the voluntary offering of information, and if the company offers warranties to the authority, its penalties may be reduced.

Overall, preliminary investigations are subject to confidentiality.

55 Are ongoing authority investigations subject to challenge before the courts?

Only a deciding administrative act can be appealed and challenged before the courts. A 'deciding administrative act' is defined as one that resolves the merits of the specific case and can produce a definitive legal effect. As such, authorities' decisions to initiate preliminary investigations and request evidence are not subject to judicial control in general.

Nevertheless, if within the investigation period there is a violation of the right to a fair proceeding, or if there is an infraction of a fundamental right, the company can file a constitutional injunction, which should be resolved by the court within 10 days.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

There is no standard practice as to how a company should act in this situation. The existence of a foreign investigation does not create effects to an investigation in Colombia per se. Therefore, Colombian authorities are not obliged to follow foreign decisions, although in many cases they can be directly recognised in Colombia or through special proceedings. Nevertheless, regarding international treaties signed by Colombia, the administrative and

© Law Business Research 2021

prosecution bodies could give assistance to the foreign investigation bodies, or ask for assistance from the foreign investigation bodies.

However, in that event, the company should seek the advice of a lawyer to try to establish whether the best option is to co-operate with the authorities or to defend itself against the allegation. In some cases, double jeopardy (*non bis in idem*) could apply to the situation.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If a notice or subpoena from the authorities in Colombia seeks production of material relating to a particular matter that crosses borders, the company must search for and produce the documents in other countries to satisfy the request, unless it is impossible under the laws of the foreign country to obtain or reveal such information. The General Procedural Code establishes that when it is easier for one party to the process to prove certain facts, that party has the burden of providing the material to the authority. When the documents are in another language, they should be translated by an official translator and sent to the Ministry of Foreign Affairs for legalisation and apostilles as required by the relevant countries involved.

The costs of the translation and the time taken for the Ministry of Foreign Affairs to legalise the translation of the documents may be considered as difficulties.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Law enforcement in Colombia may share information or investigative materials with law enforcement in other countries, depending on the authority that is requesting the information. Recently Colombia has become a member of the Organisation for Economic Co-operation and Development (OECD), which has led to Colombia signing different types of agreements for the exchange of information with international authorities, mostly concerning tax requirements compliance.

There is frequently an exchange of information with international authorities when the matter concerns trust, financial, criminal and corporate authorities.

Framework for co-operation with foreign authorities in Colombia

- Foreign Account Tax Compliance Act;
- Foreign Corrupt Practices Act;
- American Convention Against Corruption;
- UN Convention Against Corruption;
- OECD Anti-Bribery Convention;
- Basle Committee (Basle III: International Regulatory Framework for banks);

© Law Business Research 2021

- Law 1474, 2011;
- Law 1712, 2014;
- Law 1778, 2016;
- Organic Statute of the Financial System;
- Decree 1848, 2016;
- External Circular 100-00011, 2021, of the Superintendence of Companies; and
- Decree 950, 1995.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

The enforcement authorities in Colombia should act according to the legal requirements regarding retention and secrecy for any type of information relating to fundamental and constitutional assets, especially when there is an ongoing judicial proceeding. Individuals can also request certain authorities (antitrust, financial, corporate and tax) to grant special confidentiality in respect of the information disclosed during an investigation.

Concerning commercial companies, an authority is only allowed to order the disclosure of commercial books and papers for the following purposes:

- appraisal of taxes;
- surveillance of credit institutions, commercial companies and institutions of common utility;
- investigation of crimes; and
- bankruptcy and liquidation of companies in both cases and of successions in the latter.

There may be partial disclosure of commercial books in a situation other than as listed above, and the authority can examine only what concerns the specific litigation.

The disciplinary code for public authorities contains a ban on allowing access to records, documents or information by unauthorised persons during and after an investigation.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A company that has received such a request should oppose the release of information establishing that the production of the content of the documents would violate the law in the other country. In this event, it is important that the company obtains a legal opinion with a translation of the support regulations, explaining why it is impossible under law to obtain, furnish or reveal that information.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Law 1581, 2012 establishes that any person who intervenes in the management of personal data is obliged to secure the confidentiality of that information.

© Law Business Research 2021

Decree 2153, 1992 establishes that natural or legal persons subject to investigations by the Superintendence of Industry and Commerce may request that any information regarding business secrecy, or information that is to be supplied during the investigation and the administrative process, be kept confidential. The company should attach a non-confidential summary of the matters included in the document to the top of the privileged document. If the authority fails to meet this request, it is liable to disciplinary penalties.

Law 1712, 2014 establishes that anyone can appeal a request for information when it involves commercial, industrial or professional secrets.

All information subject to investigation that is determined by its owners to be confidential cannot be accessed by third parties other than those who are part of the relevant judicial process.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

There is a potential risk relating to how the competent authority may interpret the behaviour of a company with regard to the compelled production of material. Nevertheless, that interpretation is not a substantive merit against the party that produces material. Private persons can also request certain authorities (antitrust, financial, corporate and tax) to grant special confidentiality to the information disclosed during an investigation.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Penalties under the Criminal Code that directors, officers or employees may face for misconduct in Colombia (depending on the crime) include:

- imprisonment;
- fines;
- seizure of goods and instruments used in committing the misconduct;
- disgorgement;
- forfeiture; or
- disqualification – for up to 20 years – from participating, directly or through a representative, in public contracting procedures such as public bids and government contracts.

Under the Criminal Procedure Code and Criminal Code, companies will be subject to a civil sanction that consists of paying for all the damage caused by the misconduct of their employees or directors, fines and disqualification from contracting with the government for up to 20 years.

© Law Business Research 2021

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

This does not apply in Colombia.

65 What do the authorities in your country take into account when fixing penalties?

When fixing penalties in transnational corruption cases, the Colombian authorities may consider a graded series of criteria for sanctions (Law 1778, 2016, Article 7), based on the following:

- the economic benefit obtained or intended by the offender by his or her conduct;
- the greater or lesser capital capacity of the offender;
- the repetition of behaviour;
- the resistance, refusal or obstruction to the investigative or supervisory action and the procedural conduct of the offender being investigated;
- the use of means or of the person interposed to hide the infraction, the specific benefits or money, the goods or services susceptible to economic valuation, or any benefit or utility, offered or delivered to a national or foreign public official, or any of the effects of the infraction;
- the recognition or express acceptance of the infraction before the decree of evidence;
- the existence and compliance of transparency and business ethics programmes or anti-corruption mechanisms within the company, in accordance with the provisions of Article 23 of Law 1779, 2016;
- the degree of compliance with precautionary measures;
- if an appropriate due diligence process has been carried out, prior to a merger, spin-off, reorganisation or acquisition of control process in which the company committing the infraction is involved; and
- if the authorities responsible for sanctioning the commission of behaviours set forth in Article 2 of Law 1778, 2016 by employees, legal representatives or shareholders have been informed in accordance with the provisions of Article 19 of Law 1778, 2016.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Under Law 1778, 2016 (administrative liability of legal entities for acts of transnational corruption), non-prosecution or deferred prosecution agreements are not available in Colombia for corporations.

© Law Business Research 2021

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Under Law 1778, 2016 (administrative liability of legal entities for acts of transnational corruption), Colombia does not provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Under Law 1778, 2016, settlements with law enforcement authorities cannot be reached through agreement or negotiation. Although Law 1778 allows the authority to grant benefits in exchange for effective collaboration, the process for obtaining those benefits is not a negotiation but rather consists of filing a request with admissions of wrongdoing and supporting evidence for the same, and the authority will unilaterally determine the effectiveness of the alleged collaboration and make its own decision.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Law enforcement authorities in Colombia do not use external compliance monitors as an enforcement tool.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

No. Access to Law 1778 files is very restricted.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under Colombia's Criminal Procedure Code (which applies only to natural persons), preliminary investigations undertaken by the prosecutor are classified. Therefore, information relating to the case will not be made public until the indictment. The Criminal Procedure Code provides that all hearings must be public. However, judges may make some exceptions in relation to the publicity of certain criminal hearings.

© Law Business Research 2021

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for companies to use a public relations (PR) firm to manage a corporate crisis, and larger companies will have their own PR and communications department. In either situation, it is also common for companies to hire criminal and compliance lawyers to work on the matter with their communications team.

73 How is publicity managed when there are ongoing related proceedings?

Ongoing proceedings are confidential until the indictment hearing. However, the media are always interested in high-profile cases, and will therefore gather confidential information, which is usually provided by the parties or authorities involved in the case.

When trials in high-profile cases begin – since they are open to the public – it is common for the media to attend.

It is also common for individuals or companies to use the media to expose their case arguments to generate positive public opinion and to try to put pressure on the authorities.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Agreements may be confidential; thus, it depends on the kind of agreement that has been reached.

However, an excerpt from the sanctioning administrative decision for transnational corruption will be published in newspapers and on the website of the sanctioned legal entity for up to one year.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Colombia does not have general obligations regarding ESG matters for companies. Nevertheless, there are some laws in respect of ESG matters, such as:

- Law 1901, 2018, which regulates some ESG matters for a particular type of corporation, namely benefit and collective interest companies (BIC). Those corporations have obligations regarding labour, environmental, human and social rights;
- guidelines from the Environmental and Sustainable Development Ministry regarding environmental management of hazardous waste; management of solid waste; sustainable production and consumption; and biodiversity;
- National Council of Economic and Social Policy (CONPES) strategy document 3527, on national productivity and competitiveness policy; and
- CONPES 3582, on national science and technology policy.

© Law Business Research 2021

Furthermore, in the few past years, a large number of Colombian companies have signed the United Nations Global Compact to enforce processes within their corporate activities that can strengthen environmental, human and labour rights, as a demonstration of good corporate practice.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Yes, the Colombian government has announced some legislative changes to comply with the guidelines stated by the Organisation for Economic Co-operation and Development in respect of ESG. Furthermore, the Ministry of Industry and Trade has announced the introduction of regulations for BIC companies that will regulate ESG processes.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

No, as Colombia is currently enforcing newly introduced ESG laws, there are no notable cases or litigation regarding the subject.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

During the next two legislative periods, we expect to see key legislative changes suggested and requested in the third phase report by the Working Group on Bribery from the Organisation for Economic Co-operation and Development, such as the approval of a law regarding criminal liability of corporations, the adoption of whistleblower protection legislation, and the reinforcement of the Superintendence of Corporations to expand the scope of its control and to establish an appropriate forfeiture mechanism for the bribery investigations process.

As a result of these changes, compliance programmes will also be more regulated and enforced by different authorities.

© Law Business Research 2021

11

France

Stéphane de Navacelle and Julie Zorrilla[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Since the Law of 9 December 2016 addressing transparency, anti-corruption and economic modernisation (known as the Sapin II Law) entered into force, 13 judicial public interest agreements (CJIPs, which are the French equivalent of deferred prosecutions agreements) have been agreed to by corporations. Since December 2020, the field of application of CJIPs has widened to include environmental crimes. In the past two years, seven CJIPs have been signed, one of which stands out.

On 9 February 2021, two companies, Bolloré SE and Financière de l'Odet SE, had signed a CJIP with the French Financial Prosecutor to settle corruption allegations pertaining to public procurement contracts for the concession of the port of Lomé, in Togo, by paying a fine of €12 million. This company is owned by Vincent Bolloré, one of the wealthiest businessmen in France.

In parallel with the CJIP, company executives and Mr Bolloré agreed to sign a plea agreement (CRPC) with the prosecutor to settle the allegations levied against them personally by each paying a fine of €375,000 fine. Although CJIPs, which are available only for legal persons, do not imply an admission of guilt, the CRPC carries the same legal effects as a criminal conviction. Both CJIPs and CRPCs, when they are concluded between a defendant and the prosecutor, must be homologated during a public hearing before a homologation judge. The homologation judge must verify that the alleged facts

1 Stéphane de Navacelle and Julie Zorrilla are partners at Navacelle. The authors thank their colleague Clémentine Duverne for her contribution to this chapter.

© Law Business Research 2021

are real, that the legal charges are justified and that the defendant acknowledges his or her guilt during the hearing.

In the *Bolloré* case, although the CJIP was homologated, the judge refused to homologate the CRPC and sent the case back to the investigating judge, who may order a subsequent trial. The homologation judge held that the alleged offences 'seriously undermined public economic order' and 'undermined Togo's sovereignty'. According to this judge, a public trial was warranted.

This case is of interest for cases of white-collar crime in which a CRPC for the executives and a CJIP for the company are negotiated. This method is supposed to afford predictability on the outcome of the case for the defendants. In the *Bolloré* case, during the public hearing, which was attended by the press, Mr Bolloré acknowledged the charges publicly and acknowledged his guilt. Despite this acknowledgement and because the homologation was refused, he is due to appear on trial most likely in 2022. This raises the question of the risks that a plea bargain in French law represents when a defendant acknowledges his or her guilt in open court during a homologation hearing as required by law, but the homologation is subsequently refused. This could be viewed as a direct breach of the subsequent right to a fair trial and violation of the presumption of innocence at the subsequent trial.

Alongside the signing of CJIPs and CRPCs, the investigative and judicial authorities in France continue to investigate corporations for offences, such as the investigation and charges of money laundering and financing of terrorism brought against global manufacturer LafargeHolcim. The manufacturer's target status was partially confirmed by the Supreme Court for which a corporate can be an 'accomplice to crimes against humanity' even if it does not intend to be associated with the commission of those crimes.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held liable on both civil and criminal grounds.

Corporate civil liability is incurred via contract or outside the framework of a contract (a tort).

Corporations can be held criminally liable for offences committed on their behalf by their organs or representatives (i.e., individuals who have executive, administrative, managerial or control functions or those who act pursuant to a valid delegation of power). Corporate criminal liability does not exclude liability of the individual having committed the offence or an accomplice to the offence, since the highest French judicial court (the Court of Cassation) gives weight to management endorsement of corporate misconduct. Although corporate criminal liability can also be found independently of individual liability, the Criminal Division of the Court has nevertheless reasserted that corporate criminal liability requires the identification of an organ or a representative.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are regulated by judicial authorities – with investigative and prosecutorial functions – but also administrative and regulatory authorities. For the most part,

© Law Business Research 2021

jurisdiction between the authorities is dependent on subject matter, with numerous opportunities for co-operation and competition.

Jurisdiction of the judicial courts is usually defined by the location of the offence or the location of the corporate headquarters.

Moreover, specialised interregional courts have jurisdiction over complex economic and financial matters, or multi-jurisdictional matters.

Furthermore, specialist sections of the prosecution authorities in Paris have national jurisdiction to handle specific offences (e.g., financial crime and corruption, terrorism and crimes against humanity). One example is the National Financial Prosecutor's Office (PNF), which investigates and prosecutes financial crimes (such as public and private corruption, favouritism, aggravated tax fraud, VAT fraud, insider trading and index fund manipulation).

Administrative and regulatory authorities also oversee the activities of corporations. The French Financial Markets Authority (AMF) regulates the integrity of financial markets, ensuring investor protection and information, and preventing market abuse. The French Competition Authority combats antitrust practices and ensures the lawful functioning of the markets by conducting field enquiries, overseeing corporate mergers, and publishing opinions and recommendations. France's Supervisory and Resolution Authority (ACPR) preserves the stability of the financial system, working with international bodies that supervise insurance and banking industry corporations' operating conditions and compliance with rules designed to protect customers. The French Anti-Corruption Agency (AFA) controls and sanctions corporations covered by Article 17 of the Sapin II Law (i.e., corporations with more than 500 employees, or a group with headquarters in France with more than 500 employees and a turnover that exceeds €100 million) for flawed or insufficient anti-corruption processes and policies, and monitors the implementation of anti-corruption programmes.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Investigations can be initiated by the public prosecutors, or by civil parties via the filing of a formal complaint with an investigating judge.

With respect to public prosecutors, investigations are initiated pursuant to complaint, reporting, voluntary disclosure or *flagrante delicto*. Prosecutorial discretion with respect to the following steps is considerable. The public prosecutor can choose to prosecute, to settle or to drop the charges, to investigate itself or to appoint an investigating judge to handle complex cases. There is no minimum threshold of suspicion provided by law for prosecutors to initiate investigative acts and the latter cannot be challenged in court.

With respect to investigating judges, investigations are initiated either through the prosecutor or pursuant to a complaint filed by civil parties. Non-governmental organisations that have been in place for a certain number of years can also file a complaint if the facts of the complaint pertain to the objective of the organisation.

Investigating judges will be seized *in rem* and their investigative acts will be limited to the facts as presented by the public prosecutors. All investigative acts of the investigating judge can be challenged in court.

© Law Business Research 2021

Investigations can also stem from administrative or regulatory authorities' detection of suspicious activities within their material jurisdiction (e.g., AMF, AFA, ACPR).

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Orders issued by investigating, administrative and judicial authorities must comply with specific formalities and be based on a legal provision.

Notice to attend or a subpoena (i.e., a written notice that requires a party to attend a court hearing or to produce a document to the authorities) can be challenged under French law if the orders are not provided for by law or do not contain the appropriate information to inform the recipients of their rights.

Moreover, the principle of secrecy (e.g., professional secrecy, bank secrecy, defence and security), for instance, is a ground to object to the issuance of an order for the communication of documents – even though the trend in recent case law has admitted the seizure of documents protected by the attorney–client privilege.

When a notice or a subpoena is issued by a foreign authority, it is possible to challenge whether it is lawful by opposing the French Blocking Statute (Law 68-678 of 26 July 1968). The French Blocking Statute prohibits any request for or submission of information or documents of an economic, commercial, industrial, financial or technical nature, whether in writing or orally, either affecting the essential economic interests of France or in view of the information or documents constituting evidence in foreign judicial or administrative proceedings outside the framework of international treaties or agreements.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

There are no formalised co-operative agreements signed with corporations that grant immunity or leniency for individuals who assist or co-operate with authorities.

Nevertheless, the co-operation of individuals with authorities could lead to more lenient sentences. Plea bargaining for individuals is only permitted should they admit guilt (a CRPC); in return, they will receive half the applicable prison sentence. Moreover, for offences relating to private and public corruption, a prison sentence can be halved should an involved individual co-operate with the administrative or judicial authorities and contribute to putting an end to the offence or identifying the offenders or accomplices.

7 What are the top priorities for your country's law enforcement authorities?

For several years, in the field of financial crime, the main priority for French enforcement authorities has been the fight against corruption.

This priority was reaffirmed by the Criminal Policy Circular issued by the Minister for Justice on 2 June 2020, which focuses on the fight against international corruption and was adopted in the wider context of the Organisation for Economic Co-operation and Development's assessment of the anti-corruption arsenal in France. This is also evident

© Law Business Research 2021

in the interest shown in a report by two Members of Parliament on an evaluation of the Sapin II Law (the Gauvain/Marleix Report) and the subsequent bill to improve it.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Within the context of a trial for probity offences, corporations meeting the requirements of the Sapin II Law, under Article 17, can request the public prosecutor to offer a CJIP and to impose a lower financial sanction. Nevertheless, this remains at the public prosecutor's discretion.

The public prosecutor considers the ability and willingness of the executive management, once it is aware of the offences that have been committed within the corporation, to implement the necessary corrective measures to enhance the compliance programme. Implementing an effective corporate compliance programme may be a condition of a CJIP and the law enforcement authorities can order the AFA to monitor the compliance programme of a corporation for up to three years.

In practice, should a company enhance its compliance programme in accordance with best practice before a CJIP is signed, the public prosecutor may rule on completion of the structure of the programme, and the AFA will only have to monitor its implementation.

The first official guidance on the content of an effective compliance programme was provided by the eight pillars of the Sapin II Law, namely code of conduct, whistleblower channel, risk mapping, due diligence on customers, suppliers and third-party agents, internal and external accounting controls, training for high-risk employees, disciplinary sanctions, and monitoring and evaluation of measures. Moreover, the AFA has issued several sets of guidelines – including Practical Guide on the Corporate Anti-Corruption Compliance Function and Practical Guide on Implementation of the Compliance Programme Sanction – and practical Q&As for private and public sector entities.

Although AFA recommendations are not legally binding, compliance with them is taken into consideration in the event of subsequent control measures.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

A comprehensive framework addresses cybersecurity at different national levels.

The National Cybersecurity Agency (ANSSI), established in 2009, is the national authority in charge of cyber-defence and information security. Its purpose is to oversee the activities of government departments, public services, strategic businesses and operators, with the aim of providing a proactive response to cybersecurity matters. It also issues authorisations for exports and imports of goods containing encryption. Alongside ANSSI, other specialist bodies address cybersecurity: the police force (Central Cybercrime

© Law Business Research 2021

Prevention Office) is responsible for fighting crimes linked to information and communication technologies, the National Gendarmerie office is responsible for fighting digital crimes and the Paris Prefecture brigade is responsible for the investigation of information technology fraud.

Should an undertaking's cybersecurity measures fall short of ensuring data protection, for instance, administrative fines can be incurred.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The implementation of cybercrime regulations is coordinated by the Interior Ministry in collaboration with ANSSI and dedicated police services. The legal framework for tackling cybercrime has grown in recent years, drawing from the Budapest Convention on Cybercrime of 23 November 2001, which harmonises national laws across Europe, improves investigative techniques and increases co-operation between European states.

Several pieces of French legislation include sanctions for offences constituting cybercrime. The Criminal Code sanctions hacking and denial-of-service attacks and the Code of Intellectual Property sanctions phishing and possession or use of hardware to commit cybercrime – offenders face imprisonment and fines up to €375,000.

French law provides for extraterritorial application of its provisions in that a cybercrime is considered to have been committed in France if the offence is committed through an e-communication network to the detriment of a person in France or a company with its registered office in France.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law can have extraterritorial effect should a crime or misdemeanour be committed abroad by a French national. For misdemeanours (*délits*) committed abroad, extraterritoriality will apply, provided that the conduct is sanctionable under the legislation of the country in which it was committed (double incrimination). In respect of corruption, whether in a public or private context, the Sapin II Law removes the double incrimination requirement and extends the extraterritoriality effect to French residents or those individuals and corporations who conduct their economic activity on French soil.

Criminal law can also have extraterritorial effect should a crime or misdemeanour that is sanctioned by imprisonment be committed abroad against a French national.

The public prosecutor can only initiate proceedings against an offender once a formal complaint has been filed by a victim or by the concerned foreign authorities.

In specific circumstances, French criminal law can have extraterritorial effect should a crime or misdemeanour be committed abroad by a non-French national, in the event that his or her extradition or transfer to his or her country of origin is refused by the French authorities.

© Law Business Research 2021

French criminal law can also have extraterritorial effect in other limited circumstances, such as when the fundamental interests of the nation, diplomatic or consular agents or premises are targeted and when crimes and misdemeanours pertaining to acts of terrorism are committed abroad by a French national or a resident on French soil.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The challenges of cross-border investigations mainly occur when the French authorities are not involved in the investigation and prosecution proceedings.

The United States has always encouraged a more hard-line enforcement of international financial and corruption issues globally, whereas the French authorities tend to co-operate with the United States without tackling the issues proactively and independently. The Sapin II Law marks the change in cross-border investigations, in which the French authorities are much more involved and trusted as international participants. The *Airbus* CJIP (judicial public interest agreement) is an illustration of this new status. The National Financial Prosecutor's Office coordinated the investigations with the United Kingdom's Serious Fraud Office and the United States Department of Justice and was the main point of contact for Airbus.

Even though the French authorities are currently more involved in cross-border investigations, some issues remain. One of the main challenges is to ensure that French corporations and individuals abide by the French Blocking Statute. This statute prohibits the communication of economic, commercial, industrial, financial or technical documents or information to foreign authorities or the use of any such information as evidence in legal proceedings abroad, subject to mechanisms afforded under international agreements or treaties, such as the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention) or a mutual legal assistance treaty.

To mitigate this challenge when the French authorities are not involved in a request for communication from foreign authorities, French corporations or individuals can seek advice from the French Anti-Corruption Agency or the Strategic Information and Economic Security Service of the Ministry for Economy and Finance.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The principle of double jeopardy enshrined in Article 14.7 of the International Covenant on Civil and Political Rights, Article 50 of the Charter of Fundamental Rights of the European Union and Article 4 of Protocol No. 7 to the European Convention on Human Rights has been ratified by France. The French state provides an exception in its ratification of Article 4 of Protocol No. 7, limiting the application of *ne bis in idem* to the field of

© Law Business Research 2021

criminal law. Based on this principle, no individual who has been convicted or acquitted in France by definitive criminal judgment may be prosecuted again for the same offence.

French criminal case law considers, however, that *ne bis in idem* does not apply when a definitive foreign judgment has been rendered for an offence of which elements occurred in France. For instance, on 14 March 2018, in a decision regarding the Oil-for-Food Programme, the Court of Cassation (the highest criminal court in France) confirmed that Article 14.7 of the United Nations International Covenant on Civil and Political Rights applies only when both proceedings are initiated in a territory of the same state. Thus, the double jeopardy provision found in a US deferred prosecution agreement (DPA) does not apply.

Owing to the French exception in its interpretation of Article 4 of Protocol No. 7, it is possible in France for an individual or corporation to be sanctioned for the same offence by both judicial and administrative authorities. On 6 June 2019, however, in a case involving two sanctions for market offences – by the French Financial Markets Authority and the criminal court – France was convicted by the European Court of Human Rights (ECHR) for violation of the *ne bis in idem* principle (*Nodet v. France*, Case No. 47342/14). The ECHR called on France to ensure that each proceeding is duly considered and that the overall amount of all penalties is proportionate.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are a recent development in France in multi-jurisdictional investigations. The *Société Générale* CJIP in 2018 and the *Airbus* CJIP in 2020, both signed alongside foreign DPAs, demonstrate an intent to reinforce co-operation between cross-border authorities. The main practical consideration with respect to global settlements is that they can occur in jurisdictions with an entirely different legal system.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

In criminal matters, save for cases in which *ne bis in idem* applies, the French authorities are free to take a foreign court ruling into consideration to open an investigation. The French authorities conduct their own investigations independently.

In practice, however, the emerging trend is towards co-operation between French and foreign authorities.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The implementation of economic sanctions in France is essentially part of UN sanctions policy and the EU Common Foreign and Security Policy. Restrictive measures, such as asset freezing, embargoes and commercial restrictions, are enforced by a European Council decision supported by EU Regulations and are directly binding on EU Member States. Unilateral measures can also be implemented by national decree or order, even though the

© Law Business Research 2021

European Commission, in a recent non-binding opinion, has considered unilateral asset freeze measures to be incompatible with EU law.

The sanctions may target governments of foreign countries, non-government entities and individuals. France's Ministry of the Economy and Finance (Directorate-General of the Treasury) and Ministry for Europe and Foreign Affairs oversee the implementation of any sanction decided at European level.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

There is no unique approach to sanctions enforcement.

In recent years, measures to fight terrorism financing have increased. For instance, the French Monetary and Financial Code entitles the Minister of Economy and Finance to order the freezing of assets belonging to individuals or legal entities who commit, or attempt to commit, terrorist acts, or who facilitate or participate in such acts. On 17 June 2019, the French Directorate-General of the Treasury published an updated version of the guidelines drafted with the Supervisory and Resolution Authority on the implementation of French economic sanctions.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

There is no general framework to criminalise the violation of economic sanctions, although a bill for this purpose was considered by the French Parliament in 2016. However, France enforces international and European restrictive measures.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

As a member of the European Union, France is subject to the EU Blocking Regulation established on 22 November 1996 and updated on 6 June 2018 by the European Commission. This Regulation is directly enforceable in France. The measure forbids EU citizens from complying with third-country extraterritorial sanctions unless exceptionally authorised to do so by the European Commission, as set forth in Commission Implementing Regulation (EU) 2018/1101. A case concerning the interpretation of the EU Blocking Statute and its effects on US sanctions is currently pending before the Court of Justice of the European Union (C-124/20), and is apparently still ongoing.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Although the EU Blocking Regulation sanctions EU companies that would comply with third-country sanctions, the measure has much more of a symbolic effect than an economic one.

© Law Business Research 2021

It has been applied only in 1998 in the context of a complaint filed by the European Communities before the World Trade Organization. As regards the US sanctions on Iran, experts are sceptical about how far Europe will ultimately go to enforce such a rule. It could also prove difficult to enforce, in part because of the international banking system and the significance of the United States in international financial markets.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations can come to light through various channels.

Article 8 of the Sapin II Law provides for a three-tiered reporting system, by which employees or business partners first must submit an alert to their direct supervisor, employer or designated representative. Second – if no appropriate action is taken or there is a likelihood of imminent danger – the alert must be submitted to the relevant judicial, administrative or professional authority. Third – if no appropriate action is taken or there is a likelihood of imminent danger – the alert must be made public. Appropriate procedures for collecting reports must be established by legal entities with more than 50 employees, state administrations, municipalities with more than 10,000 inhabitants, public inter-municipal co-operation establishments, departments and regions.

INFORMATION GATHERING

22 Does your country have a data protection regime?

France adopted a data protection regime in 1978 with the Law on Information Technology, Data Files and Civil Liberties.

In 2016, the European Parliament and the Council of the European Union adopted the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. The GDPR was incorporated in France's internal legislative framework by Law No. 2018-493, which was passed on 20 June 2018, amending the existing law, of which some provisions were contrary to the GDPR.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Law No. 2018-493 of 20 January 2018 and the GDPR grant new investigating and sanctioning powers to the National Commission on Computing and Liberty (CNIL).

The right of the individual to information and the right of access, rectification and deletion of personal data are reinforced and the sanctions imposed in the event of obstruction or non-compliance with the legal provisions are increased. The CNIL has the power to impose a periodic sanction (limited to €100,000 per day) in addition to administrative fines (which can be as much as €20 million or 4 per cent of annual global turnover).

© Law Business Research 2021

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Although there are several data protection issues relevant to internal investigations in France, these are not country-specific, as they result from European regulation (i.e., the GDPR).

The main issue is that lawyers leading internal investigations may find themselves as guarantors of data protection and must reconcile this duty of protection with the duty of professional secrecy. It is necessary to clearly identify the regulations applicable to the use or transfer of data, such as the rules protecting the transfer of data considered to be within the scope of the interests of France (i.e., the Blocking Statute and rules on corporate secrecy), the rules protecting the access, processing and transfer of personal data outside or within the European Union (e.g., transfers based on international conventions), the rules protecting the rights of individuals who are subject to internal investigations (e.g., information provided to individuals regarding their right to access, rectify or delete data) and the rules pertaining to the length of time for which data can be stored.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

When employees use technological devices made available to them by their employer for professional purposes, those devices are presumed to be professional. Employers are therefore permitted to request to consult or access them. The courts, however, have curtailed this right of access based on the right to privacy. Professional emails, text messages or chat applications expressly labelled as private are thereby confidential and not accessible by the employer.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes, search warrants and dawn raids are a key element of enforcement and evidence gathering by judicial and administrative authorities.

Strict legal provisions apply to search warrants and dawn raids. The latter must be authorised either by the public prosecutor for in flagrante delicto and preliminary investigations or the investigating judge for judicial investigations. In preliminary investigations, the consent of the individuals or corporations to be raided is needed. Should consent not be given, the dawn raid must be authorised by the Judge of Liberties and Custody. Moreover, dawn raids can be conducted only between 6am and 9pm, except in cases of organised crime and terrorism. Minutes of the dawn raid are drafted and signed by the entities or individuals involved in the raid.

© Law Business Research 2021

Companies subject to dawn raids should ensure that these legal provisions are followed. Any incident should be recorded in the minutes of the dawn raid and the minutes should not be signed if there is any disagreement regarding the content.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privilege only attaches to external lawyer material and not that of in-house counsel.

Privileged material is protected from investigating and judicial scrutiny, save for materials unrelated to defence rights or those establishing the participation of the lawyer in an offence.

Corporations or individuals must thereby indicate the material that is covered by the attorney–client privilege. In the case of seizure of privileged material, the corporations or individuals involved must seek permission to make copies and file a subsequent request to have the privileged material returned.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

There are two separate regimes for witnesses and suspects.

During the investigation phase, police officers can summon as a witness any person who they deem fit for the purposes of the investigation. Should a witness refuse to comply, a police officer may notify the public prosecutor, who may compel the person by official notice. Witnesses who fail to appear or testify before the investigating judge or police officer without proper reason face a €3,750 fine. Before a court, witnesses are always compelled to attend the hearing and testify. The summons issued to a witness must also state that failure to appear, refusal to testify and perjury are punishable by law. Witnesses who refuse to appear without proper reason face a €10,000 fine.

Police officers can detain suspects for the amount of time necessary for the purposes of the investigation and under the limitations of the law and approval of a judge. A suspect can refuse to answer questions based on the right against self-incrimination.

Testimony can also be refused on account of public service (e.g., diplomatic, presidential or parliamentary immunity) or professional secrecy. Testimony revealing information of a secret nature by a person who is in possession of that information, owing to state, professional or temporary function or mission, is sanctioned by imprisonment or a €15,000 fine, save for limited exceptions.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Until the implementation of the European Whistleblowing Directive (for which the deadline in December 2021), which grants broader protection to whistleblowers

© Law Business Research 2021

(e.g., access to free information and advice about the available procedures for protection against any legal action taken against them), the Sapin II Law provides relevant protective measures.

There are no financial incentives for whistleblowers in France. The idea of a financial incentive scheme was considered but the French Constitutional Council ruled against it.

With respect to legal protections, whistleblowers cannot be excluded from recruitment procedures or professional training, cannot be dismissed, or face direct or indirect discriminatory measures. The protection of whistleblowers' identity must also be guaranteed.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Internal investigations do not benefit from a dedicated legal framework. In September 2016, the Paris Bar adopted a *vade mecum* of ethical recommendations for investigating lawyers, which was amended in December 2019. On 12 June 2020, the National Council of Bars also published a guide for French lawyers conducting internal investigations. Other legal provisions apply to these internal investigations.

Employees whose conduct is within the scope of an investigation could benefit from several rights, but these are not expressly provided by law. Employees interviewed within an internal investigation should be informed that the external lawyer represents the company and not their personal interests and that they can be assisted by an independent lawyer, should their conduct amount to misconduct. The purpose of the interview and its non-coercive nature should also be indicated.

Furthermore, data protection and privacy laws apply to all employees regardless of allegations of wrongdoing, allowing employees to access and modify all personal data that has been collected and entitling them to invoke the right to privacy. This right to privacy may be circumvented, however, should emails, text messages or chat applications be located on professional devices, and they are not marked as private or in a private inbox.

There is no different treatment applicable to officers and directors of companies within internal investigations.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Presumption of innocence applies to all employees, including those who are deemed to have engaged in misconduct. These employees thereby benefit from the same rights as other employees (e.g., notice for interview and notification of rights). Employees suspected of misconduct must be advised of their right to a lawyer.

If misconduct is confirmed, an employer has several options for sanctioning employees, including dismissing them or putting them on furlough during the investigation.

© Law Business Research 2021

32 Can an employee be dismissed for refusing to participate in an internal investigation?

The labour courts appear to consider the refusal to participate in an internal investigation as a sufficiently severe fault to warrant sanction under specific circumstances.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

When judicial review by a labour court is likely to happen (e.g., if an employee who has been sanctioned for misconduct challenges the findings of an internal investigation), it is considered best practice to prepare a document setting out the terms of reference or investigatory scope before commencing an internal investigation.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

French law does not provide a clear set of rules with respect to the steps a company should take internally when it becomes aware of an issue with legal implications. The company should assess the scope of the facts and the probability of incurring liability, to determine the interest in co-operating with the authorities and to set out a defence strategy.

There is no obligation to report back to authorities, but this is encouraged within the framework of a CJIP (judicial public interest agreement). The joint guidelines issued by the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF) (the AFA-PNF Guidelines) on the implementation of CJIPs expressly provide, however, that voluntary self-disclosure by a company will be taken into account favourably, both for the opportunity to settle a CJIP and as a mitigating factor.

The main legal requirement is for individuals or corporations not to destroy or amend evidence.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is very likely that the enforcement authority would collect documents or data directly by carrying out a raid within the company, having gathered sufficient information from third parties to ensure that it is possible to collect relevant information. If a company has any reason to believe a raid is likely, it should immediately ensure that any documents that may be seized indicate privilege, where relevant.

Administrative authorities (e.g., AFA, the French Financial Markets Authority, the Supervisory and Resolution Authority and the Competition Authority) can request

© Law Business Research 2021

communication of data and documents from companies under review or directly from third parties. If these requests are legally permitted, corporations must comply.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Other than those attached to publicly traded companies, there are no obligations as to when a company must disclose the existence of an internal investigation or contact from a law enforcement authority.

Self-disclosure is an option available to obtain credit for co-operation.

37 How are internal investigations viewed by local enforcement bodies in your country?

Influenced by the Anglo-Saxon legal culture, internal investigations have been progressively accepted by specialist financial investigating judges and prosecutors.

Although negotiating a deal with a prosecutor or an investigating magistrate is still rather uncommon, the number of CJIPs has increased in recent years, and internal investigations are an effective tool in multi-jurisdictional matters and cross-border negotiated justice. French authorities are relying more and more on internal investigations, which are considered a key component of a criminal file.

Pursuant to the AFA-PNF Guidelines, should a company be interested in concluding a CJIP, it is encouraged by the prosecution authorities to demonstrate its co-operation by disclosing the findings of any previous or current internal investigation.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

There is no attorney–client privilege for communications with in-house counsel in France. To benefit from privilege, investigations should be carried out by external lawyers. Lawyers cannot be freed from the duty of professional secrecy under any circumstances, even by their clients.

Professional secrecy applies between lawyers and their clients but not with the employees of their clients. Lawyers must therefore notify those employees that anything they say can be disclosed to the authorities by their employer. Confidentiality applies to communications between lawyers and providing separate counsel to individuals is recommended to facilitate safe communications.

The joint guidelines issued by the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF) (the AFA-PNF Guidelines) differ slightly from the Paris Bar's *vade mecum* for investigating lawyers, published in 2019. Whereas the AFA-PNF Guidelines state that not all the evidence included in an internal investigation report is necessarily covered by lawyers' professional confidentiality, the *vade mecum*

© Law Business Research 2021

provides that all documents drawn up by lawyers in the course of their work are covered by professional secrecy.

In any case, the client is at liberty to disclose documents.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There is no specific attorney–client privilege relating to corporations.

The particularity within this context is to determine who the counterpart of the lawyer is within a corporation, which will usually be the general manager or general counsel.

There are no differences when the client is an individual.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

There is no privilege attached to communications with in-house counsel. Privilege only attaches to external lawyers.

The Gauvain Report on the Protection of French Companies Against Extraterritorial Laws and Measures published on 26 June 2019 recommends introducing privilege applicable to legal advice given by in-house counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

There is no general provision regarding the attorney–client privilege as regards foreign lawyers in relation to investigations.

The Paris Bar Council has stressed that email exchanges between a client and a foreign lawyer can be covered by the attorney–client privilege. In addition, foreign lawyers can be temporarily and occasionally authorised to practise consulting and counselling activities in France. In that case, they are bound by both their home country's professional rules and the ethics rules applicable to French lawyers, which include the attorney–client privilege.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The attorney–client privilege cannot be waived by lawyers under any circumstances, even when permitted by the client, save for the personal defence of lawyers in a case opposing their client or specific cases provided by law.

The client is not bound by the attorney–client privilege.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

This concept does not exist in France.

© Law Business Research 2021

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

As the attorney–client privilege is general, absolute and unlimited in time under French law, it must be maintained, even after a limited disclosure abroad.

Co-operation between enforcement authorities is likely, however, to make the privilege moot.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privileges do not exist per se in French law. It is possible, however, for the purposes of defending a client, to share privileged information with other attorneys without waiving privilege – whether the clients share a common interest or not (*foi du palais*).

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Professional secrecy can be extended to experts on whom lawyers rely for the purposes of their work.

It is usually safer to have the information collected and processed within the law firm's offices.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no legal provisions regarding internal investigations, including the interviewing of witnesses.

Interviews with individuals who are not current or former employees of the company are not prohibited by the Paris Bar *vade mecum*, but recourse to external counsel is advised.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Professional secrecy applies between lawyers and their clients. A company can thus claim the attorney–client privilege over internal witness interviews or attorney reports. Nevertheless, the joint guidelines issued by the French Anti-Corruption Agency and the National Financial Prosecutor's Office differ slightly from the Paris Bar *vade mecum* for investigating lawyers regarding the documents covered by the attorney–client privilege.

© Law Business Research 2021

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no legal provisions regarding internal investigations, including the interviewing of witnesses.

The Paris Bar *vade mecum* makes no distinction between interviews carried out with employees and third parties.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Lawyers conducting interviews must explain to whom the attorney–client relationship applies (i.e., that they are acting in the interests of the corporation, not the employees) and that independent representation is possible. Lawyers must also indicate the purpose of the interview and its non-coercive nature.

Documents can be provided ahead of time. This practice usually occurs when an employee has separate representation. Documents are communicated from the lawyer of the company to the lawyer of the employee, as correspondence between attorneys is covered by default by privilege.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Except for specific crimes that are inchoate and can be avoided, only civil servants have a general obligation to report crimes of which they become aware in the context of their employment.

There is no legal requirement to self-report.

The guidelines on CJIPs (judicial public interest agreements) clearly state, however, that voluntary self-reporting of offences to prosecutors, if made in a timely manner – both as regards the choice of the CJIP procedure and as a factor reducing the amount of the public interest fine – will be considered favourably.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting is not very common in France.

A corporation will be advised to self-report (provided misconduct is established without doubt, proper corrective measures have been taken and the corporate compliance programme has been reinforced) to be eligible for credit for co-operation with the judicial authorities notified of the misconduct. The involvement of foreign authorities can also

© Law Business Research 2021

have a bearing on a decision to self-report, as well as the multi-jurisdictional aspect of investigations, should the multiple authorities involved be likely to collaborate.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no specific procedure for self-reporting and no legal requirement to do so.

Informal contacts should be made, through external counsel, with the competent authority, after a thorough analysis of the advantages and disadvantages. Although there is no statutory requirement to evaluate self-reporting and co-operation in a CJIP, the joint guidelines issued by the French Anti-Corruption Agency and the National Financial Prosecutor's Office indicate that self-reporting within a reasonable period shall be considered favourably, as a factor for encouraging the offer of a CJIP or reducing the fine.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Corporations must respond in writing to notices or subpoenas from a law enforcement authority in compliance with the methods and time limits provided by law.

It is possible to enter into dialogue with the investigating authorities, whether the investigating judge or the public prosecutor, but these communications often remain unofficial and may not amount to anything. Alongside ad hoc communications, investigative acts beyond the scope of the mandate of the judicial authority can be challenged in court.

55 Are ongoing authority investigations subject to challenge before the courts?

Yes, ongoing authority investigations can be challenged before the courts.

Ongoing investigations led by a public prosecutor are not subject to challenge before the courts, except for a limited number of investigative acts that breach legal requirements. Challenges are only possible once the investigation is closed by requesting the nullity of the investigative acts.

However, investigative acts in ongoing investigations led by an investigating magistrate can be challenged before the courts.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The company should answer to all the authorities involved separately, as the questions that can be raised by different authorities vary.

It should nevertheless be borne in mind that authorities communicate with one another.

© Law Business Research 2021

When dealing with foreign authorities, the EU Blocking Statute, specific secrecy provisions, and privacy and data protection issues should also be addressed.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The collection of material abroad will have to be carried out in compliance with the applicable foreign law.

The difficulty may be that the applicable foreign law does not allow the seizure and production of material. If a corporation finds it impossible to provide requested material, it must explain the situation to the French authorities.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Co-operation with foreign enforcement authorities is increasing, both within the European Union and beyond, namely through mutual legal assistance treaties, agreements between regulators and enforcement authorities, and EU co-operation agreements.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Except where the law provides otherwise, inquiry (i.e., under an investigating magistrate) and investigation (i.e., under a public prosecutor) proceedings are confidential. Third parties are not bound by this confidentiality.

Any person contributing to an investigation is bound by this confidentiality, namely the judges in charge of the investigation, the public prosecutor, the law clerks, the bailiffs, the police investigators, the personality investigators and any interpreters or experts.

Lawyers are not bound by this confidentiality but are bound by professional secrecy. The disclosure of confidential information by breaching confidentiality or professional secrecy can be sanctioned by imprisonment for one year and a €15,000 fine.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The corporation should retain external counsel to obtain a legal opinion on the law of the country in which the documents sought are located. Co-operation with the French and foreign authorities – and perhaps with the diplomatic authorities of both countries

© Law Business Research 2021

pursuant to formal co-operation agreements – may be necessary for the production to be carried out appropriately.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Yes, France has both a country-specific blocking statute and privacy statutes.

The French Blocking Statute prohibits the communication of economic, commercial, industrial, financial or technical documents or information to foreign authorities or their use as evidence in judicial or administrative proceedings abroad, subject to mechanisms afforded under international agreements or treaties, such as the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention) or a mutual legal assistance treaty. Data protection legislation, in that it can prohibit the transfer of data outside Europe, could also constitute a type of blocking statute.

Several secrecy laws exist, depending on the interests at play (e.g., banking, security and defence, medical, journalism source or corporate secrecy). To ensure the preservation of these secrecy provisions, communications should be properly addressed when responding to a foreign authority.

Bank secrecy, for instance, should be addressed when a notice or subpoena concerns a financial institution. These institutions owe a legal duty to their customers not to disclose information about their affairs to third parties. Any banking institution that discloses information about customers faces criminal sanction pursuant to the Monetary and Financial Code and the Criminal Code.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production is limited to very specific circumstances, namely when foreign authorities are involved or there is a strategic interest in doing so in an ongoing investigation.

All material produced is included in the criminal file and is accessible, under limited circumstances, to defendants (indicted and assisted witnesses) and civil parties. Although legal professionals are bound by professional secrecy, they are not bound by the confidentiality of the inquiry. They are free to share information – not documents – from the file with their clients, who can then share the information with third parties.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Corporations sanctioned for misconduct can face fines, payment of civil compensation to victims, disgorgement of profits resulting from the offence, dissolution, publication of the sanction in the press and debarment from bidding for tender for certain specific offences.

© Law Business Research 2021

Individuals sanctioned for misconduct can face fines, imprisonment, payment of civil compensation to victims or a ban on undertaking specific managerial positions. Directors, officers or employees also face sanctions by their company, including dismissal.

Hearings are rarely closed. Therefore, corporations and individuals face the risk of having their identity disclosed in the press.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The EU Directive on public procurement has been transposed into French law, prohibiting companies found guilty of specific offences (e.g., corruption, fraud, money laundering, terrorism or embezzlement and misappropriation of property) from bidding in public procurements throughout the European Union for five years – unless the sentencing decision specifically provides for a more limited period.

French law provides that corporations cannot bid for public procurements if they have previously been sanctioned definitively by a court of law for certain offences, namely corruption, extortion or probity offences.

65 What do the authorities in your country take into account when fixing penalties?

The principle of personalisation of a sanction applies in France to corporations and individuals.

Regarding the CJIP (judicial public interest agreement) public interest fine, the joint guidelines issued by the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF) (the AFA-PNF Guidelines) specify that the fine should reflect the illegal profits derived by the corporation from the offence but can also have a punitive dimension. With respect to the punitive aspect, the AFA-PNF Guidelines consider the corruption of a public official, the fact that the legal entity falls within the scope of the compliance obligation of the Sapin II Law, the existence of possible convictions or sanctions for similar offences, any attempt to conceal the offence, and the repeated or even systemic nature of corruption. Gains in market share or increased visibility may also be considered when determining the amount of the fine.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

The French legal system does not offer non-prosecution agreements.

The CJIP (judicial public interest agreement) is available, allowing corporations accused of corruption, probity offences, tax fraud or environmental crime to settle allegations. This will imply a financial fine, without constituting an admission of guilt – thereby allowing corporations to continue bidding for public procurements – except in cases following an inquiry.

© Law Business Research 2021

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no correlation in French law between a settlement with a corporation and criminal proceedings regarding individuals. There are therefore no reporting restrictions or anonymity for corporates beyond the confidentiality of criminal settlement negotiations.

The joint guidelines issued by the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office provide that the aim of internal investigations conducted by a prosecuted company, and communicated to the prosecutor, is also to determine individual liabilities.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

If a case is likely to involve foreign jurisdictions, companies should assess the consequences of admitting guilt in France, namely regarding the principle of *ne bis in idem*.

Corporations should also be mindful that signing a French plea bargain – as compared with signing a CJIP – amounts to an admission of guilt, thus preventing them from bidding for public tenders.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Law enforcement authorities cannot use external corporate compliance monitors as an enforcement tool, as the AFA constitutes the official compliance monitor, with a monopoly on the supervision of the compliance programmes of legal entities that have signed a CJIP, in accordance with the Sapin II Law.

In specific cases, the legal entities have recourse to experts (e.g., law, accounting or audit firms) to process the AFA requests.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Should alleged victims demonstrate legal standing, they will be allowed to join the criminal procedure as civil parties and, as such, will be granted access to the criminal file and be able to submit requests for investigative acts.

Moreover, alleged victims can initiate a criminal investigation by filing an official complaint to that effect.

Private parties do not normally have access to the investigation files held by administrative authorities.

© Law Business Research 2021

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Investigations led by a prosecutor or investigating judge are confidential.

As defendants and victims have access to the criminal file but are not bound by secrecy, it is sometimes very difficult to keep communications and information confidential. To prevent leaks of fragmented or inaccurate information or to avoid disrupting public order, the public prosecutor may, either *ex officio* or at the request of the investigating court or the parties, communicate on objective elements of the proceedings, without making an assessment on the charges.

Members of the press can be present and cover the hearing – albeit microphones and cameras are not allowed in the courtroom. Defendants and victims are free to make statements within the limits of the freedom of expression.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common to have press releases, communications and crisis management strategies prepared and, when appropriate, public relations firms assisting. The spokesperson is often a lawyer on the case, especially when individuals are involved.

73 How is publicity managed when there are ongoing related proceedings?

Publicity is part of the overall strategy, namely in high-profile matters that attract political attention and have numerous civil parties.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

There are no circumstances in which a judicial settlement could be agreed privately. CJIPs (judicial public interest agreements) and plea bargains offered by public prosecutors are officially approved by judges by way of a public hearing. Moreover, CJIPs are published on the French Anti-Corruption Agency's website.

There is no obligation to disclose settlements with administrative authorities to the public.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Partially. The French Duty of Vigilance Law (enacted in 2017) requires major companies (with 5,000 employees in France or 10,000 employees worldwide) to establish, publish and implement a vigilance plan with the aim of identifying and preventing serious violations of human rights and fundamental freedom resulting from the company's activities,

© Law Business Research 2021

from activities of its subsidiaries, its subcontractors and its suppliers, or from entities with whom the company has an established commercial relationship.

There are five mandatory actions that companies must implement as part of their vigilance plan:

- a risk-mapping that identifies, analyses and ranks risks of serious violations of human rights and fundamental freedom;
- evaluation procedures that regularly assess, in accordance with the risk-mapping, subsidiaries, subcontractors or suppliers with whom the company maintains an established commercial relationship;
- appropriate actions to mitigate risks or prevent serious violations;
- an alert mechanism that collects potential or actual risks. This alert mechanism must be implemented in collaboration with trade unions organisations represented within the company concerned; and
- a monitoring scheme assessing the effectiveness of the measures put in place by the company.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

There could be developments at a European level given that, on 10 March 2021, Members of the European Parliament (MEPs) have adopted, in plenary session, the legislative initiative report with recommendations for a directive on corporate human rights due diligence.

Under the MEPs' proposal, companies would be required to identify, assess, prevent, cease, mitigate and monitor potential or actual adverse impacts on human rights, the environment and good governance in their activities and value chain.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

So far, a few cases have been brought before courts using the Duty of Vigilance Law. In that regard, owing to the lack of a public body acting as regulator, the enforcement is conducted by a few proactive non-governmental organisations (NGOs). One notable case pertains to Total, which was sued by NGOs for its lack of a vigilance plan, which the company is required to establish under the Duty of Vigilance Law.

However, uncertainties as to the content of the Law and procedural issues of jurisdiction means that it still remains difficult to ascertain what the impact of the Law will be on companies.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

France is proactive – various publications indicate regulatory and legislative amendments for the coming years.

An evaluation of the Sapin II Law's effectiveness by a commission led by two Members of Parliament, which led to a bill being introduced in Parliament in November 2021,

© Law Business Research 2021

confirms France's intent to efficiently reduce corruption and the paramount importance internationally of the National Financial Prosecutor's Office. The *Airbus* CJIP (judicial public interest agreement) in a corruption case opens the way to negotiated justice – encouraging self-reporting and full co-operation, including with foreign authorities.

The aim of the Gauvain Report on the Protection of French Companies Against Extraterritorial Laws and Measures is to restore French and European sovereignty and protect companies from extraterritorial control. It provides recommendations to reinforce the French legal framework applicable to foreign procedures targeting French companies, including strengthening the French Blocking Statute, introducing legal privilege for in-house counsels and protecting data from the US Cloud Act by the threat of fines similar to those applicable to violations of the General Data Protection Regulation.

Finally, as of 2021, CJIPs can be implemented for environmental crimes.

© Law Business Research 2021

12

Germany

Eike Bicker, Christian Steinle, Christoph Skoupil and Marcus Reischl[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The diesel emissions cases involving several German carmakers continue to be the highest-profile corporate investigations in Germany. The automotive industry is one of Germany's key industries and, therefore, the emissions investigations against several major German car manufacturers have attracted a lot of public attention. Furthermore, the high volume of damage allegedly suffered by customers, investors and others, and the technical and regulatory complexity of the topic, are notable. The criminal investigations by various German public prosecutor offices are focused on the individual criminal liability of managers, including former chief executive officers, while at the same time leading to fines of hundreds of millions of euros against the companies involved.

2 Outline the legal framework for corporate liability in your country.

Companies are technically not criminally liable under existing German law. A strict corporate criminal liability had been under discussion for the past few years but was set aside because of the federal elections in autumn 2021. It remains to be seen whether a bill on corporate criminal liability will be taken up again under a new government.

Currently, companies whose employees have committed criminal or administrative offences face the risk of an administrative fine or a confiscation order. Administrative fines are capped at €10 million, though this amount can be – and, in practice, frequently

1 Eike Bicker, Christian Steinle and Marcus Reischl are partners and Christoph Skoupil is an associated partner at Gleiss Lutz.

© Law Business Research 2021

is – exceeded by the financial benefit the company has obtained from committing the offence (i.e., profit disgorgement).

This legal mechanism (administrative fines plus profit disgorgement) has led to quite significant fines in the past, as in the *Siemens* (€395 million), *MAN* (€150 million), *Ferrostaal* (€140 million), *Volkswagen* (€1 billion) and *Audi* (€800 million) cases.

As an alternative to an administrative fine, a confiscation order can be imposed on a company if an unlawful act has been committed. The maximum amount for a confiscation order is the entire gross value of the proceeds from the respective criminal offence, and the fined party (i.e., the company) is not permitted to deduct any costs it incurs.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Various law enforcement authorities, at both federal and state levels, regulate corporations, including, among others, the public prosecutors' offices, antitrust authorities, tax authorities, financial regulators and customs authorities.

The matter of jurisdiction between the authorities depends on the scope of the potential investigation. To this extent, various areas of responsibility are assigned to specialist authorities. It is important to understand that all 16 German states have their own prosecutors, and thus some of them are more active in prosecuting corporations (e.g., Munich, Frankfurt and Stuttgart) than others.

There are no guidelines for the investigation of corporations in the form of laws or legal regulations. However, we are aware of some internal guidelines drafted to assist authorities when investigating corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The local public prosecutor's office is generally obliged to take action in relation to all prosecutable criminal offences, provided there are sufficient factual indications (or initial suspicion). However, this duty of legality pertains only to criminal offences. Therefore, the public prosecutor has discretion whether to open administrative proceedings against a corporation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Enforcement measures taken by authorities against suspects or witnesses (e.g., search warrant or confiscation) can be subject to, inter alia, judicial review. This applies to the order itself as well as the manner of execution.

Subpoenas as such are not challengeable. However, potential enforcement measures or court decisions following a subpoena may be challenged. In German criminal proceedings, the defendant is not obliged to co-operate with the authorities or to provide information about evidence-relevant facts.

© Law Business Research 2021

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Generally, the public prosecutor cannot grant immunity or leniency to individuals who assist or co-operate with investigations. However, prosecutors and courts regard co-operation as a major factor in determining the level of sentences. Furthermore, in certain cases, prosecutors have some discretionary powers to dispense with the prosecution with the consent of the accused and the court, and co-operation is certainly a factor in this decision.

The German antitrust authorities can grant immunity from fines or a reduction of fines to cartel participants who co-operate and thereby contribute to uncovering a cartel. This leniency programme is available to individuals as well as companies. Full immunity will be granted to cartel participants if they are the first to disclose the cartel and fully co-operate with the antitrust authority throughout the proceedings.

7 What are the top priorities for your country's law enforcement authorities?

Corporations in Germany are most severely prosecuted for antitrust violations and corruption. The highest fines are regularly imposed in both these areas. In the recent past, fraud and tax fraud proceedings have also been a priority (for instance, alleged irregularities regarding diesel engine emissions and cum-ex or cum-cum trading patterns of banks and financial institutions). We expect data protection violations and the betrayal of business and company secrets to attract more enforcement activity as a result of stricter legal regulations and increased sanctions.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Investigating authorities are increasingly focusing on (1) how a company's compliance programme is designed and implemented and (2) whether the company adapts its compliance measures adequately after becoming aware of potential irregularities.

Both these factors are taken into account by the enforcement authorities, in particular in their discretion as to whether and to what extent sanctions are imposed on the company.

The Federal Supreme Court confirmed this practice and ruled that investments in compliance and enhancing a compliance management system prior to and after misconduct being detected must be taken into account when setting a fine.

However, there is no official guidance on what an effective compliance programme should contain from the perspective of German authorities. German companies usually adhere to international compliance standards.

© Law Business Research 2021

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Since 2015, the issue of cybersecurity has been addressed by various laws and regulations in both German and European legislation, including the German IT Security Act, the EU Directive on Network and Information Security and the EU Cybersecurity Act. This legislation addresses the cybersecurity landscape without imposing any specific duties on individuals or companies.

Under the EU General Data Protection Regulation, companies that are processing personal data must implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risk. A violation of this duty can trigger administrative fines and claims for damages. As regards data breaches, companies may be obliged to notify supervisory authorities and the individual data subjects.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime (i.e., criminal activities carried out using computers or the internet) is covered by general German criminal law pursuant to a variety of specific provisions regarding data espionage, computer fraud, data forgery, deception in the context of data processing and data tampering.

Cybercrime investigations are seldom only national in scope. They call for coordinated action at international level and require a high level of cross-border co-operation. As an EU Member State, Germany is a signatory to the Convention on Cybercrime, which includes provisions on international co-operation with other EU Member States and further signatories, such as the United States, Japan and Australia.

On the practical side, law enforcement authorities have implemented cross-border communication networks and coordination units, including the Interpol Global Complex for Innovation, the European Cybercrime Centre at Europol and others.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

German criminal law is generally applicable if either the offender acted in Germany or the offence had a consequence in Germany. Furthermore, in 1999, Germany implemented the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of the Organisation for Economic Co-operation and Development. Since then, the German Criminal Code prohibits illicit payments to foreign public officials, in a similar way to the US Foreign Corrupt Practices Act and the UK Bribery Act. In addition, bribery payments in the private sector that exclusively affect foreign competition are covered by German law.

© Law Business Research 2021

Furthermore, German criminal law is applicable, among other reasons, if the offence is committed abroad against a German or if a German commits an offence abroad and the act is a criminal offence also in the place where the offence was committed.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations generally demand a high level of sensitivity with regard to the different expectations of the authorities involved and the different legal frameworks applicable to investigative steps in different countries.

If an investigation has links to a common law jurisdiction, privilege is often a topic because the principles of legal privilege differ. As the concept of pretrial discovery does not exist under German law, privilege is only relevant in relation to law enforcement authorities. Under German law, communication between a company and its legal advisers is not generally privileged, but the concept of legal privilege is limited – in most cases – to communication with the criminal defence counsel. The disclosure of separate information to public authorities does not generally put the legal privilege at risk.

To ensure that privilege is adequately protected, cross-border investigations require clear processes in line with the privilege provisions of all the jurisdictions involved.

Differences in data protection laws are relevant in cross-border investigations outside the European Union, where the General Data Protection Regulation is not applicable. In cross-border investigations, information is gathered in and transferred from and to different jurisdictions, and breaches of applicable data protection laws must be avoided.

When interviewing employees, employment law has to be observed. In Germany, broadly scoped investigative measures may require the involvement of a works council.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Companies are not protected, in principle, from sanctions in Germany after having resolved charges on the same core set of facts in another country outside the European Union (see, for example, the fines imposed against Volkswagen in the emission matter in the United States and Germany, or the fines imposed by German and other antitrust authorities in cross-border cartel cases based on the local effect in their respective jurisdictions). In addition, confiscation orders and similar measures against companies are not recognised as 'sanctions' in the sense of double jeopardy, so that companies are not yet effectively protected in this regard even within the European Union. Often, however, authorities consider a (potential) foreign sanction at their discretion when determining a (national) sanction.

© Law Business Research 2021

14 Are 'global' settlements common in your country? What are the practical considerations?

There is no legal framework for 'global' settlements under German law. However, as co-operation between authorities across borders generally increases, 'global' settlements with German authorities are generally achievable, at least to some extent. In the past, German authorities sometimes took account of foreign sanctions when determining a (national) fine (e.g., the *Siemens* case).

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

In principle, the decisions of foreign authorities have no (legal) effect on an investigation of the same matter in Germany. In some cases, however, German and foreign authorities collaborate with each other to avoid duplicate investigations.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Authorities are making increased use of sanction options (i.e., administrative fines, including profit disgorgement, and confiscation orders.) In 2018 and 2019, fines of €1 billion, €800 million and €535 million were imposed on Volkswagen, Audi and Porsche, respectively, in connection with potential irregularities regarding diesel emissions. Further, significant fines were imposed in antitrust proceedings and cases of corruption (€395 million on Siemens, €150 million on MAN and €140 million on Ferrostaal).

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Sanctions enforcement activities have steadily increased in recent years, although there are still considerable differences across the 16 German states.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

In some cases, there is co-operation between national and foreign authorities. This possibility has been codified in the form of mutual legal assistance, within the framework of which formal enquiries can be made.

In our experience, there is also an informal exchange between national and foreign authorities. However, there is often no such co-operation because of the effort involved and the sometimes low yield.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

According to German law, a boycott declaration is prohibited (this does not apply to resolutions of the United Nations, the European Union or Germany).

In addition, the EU Blocking Regulation (Council Regulation (EC) No. 271/96) applies in Germany. The Regulation prohibits all companies registered in the European Union from complying with the US legislation listed in the Annex to the Regulation (including US sanctions against Iran) unless exceptionally authorised to do so by the European Commission. Furthermore, the Regulation enables such companies to seek compensation if they suffer damage as a result of those US acts and regulations. In addition, judgments by foreign courts (in particular those of the United States) that are imposed to enforce sanctions are not recognised in the European Union.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

A violation of either national or EU blocking legislation is punishable by fines of up to €500,000. Furthermore, there is the risk that legal transactions in violation of the EU Blocking Regulation may be null and void or that violations of that Regulation may trigger contractual claims for damages by the affected business partner.

So far, the Regulation has not been applied in practice. There is no known case, therefore, in which administrative offence proceedings have been initiated for an infringement.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct come to light in many ways. In practice, investigations into serious wrongdoing are most often initiated by whistleblowers or as a side effect of running internal investigations.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Yes. Data protection law in Germany is regulated by the General Data Protection Regulation (GDPR) and the Federal Data Protection Act. Further, there are various provisions on data protection law in sector-specific legislation (e.g., the German Telecommunications Act).

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

With the introduction of the GDPR, the situation for companies in the European Union changed substantially. Previously, only a limited number of fines were imposed for data

© Law Business Research 2021

protection breaches. Now, companies can face a maximum fine of €20 million or 4 per cent of their annual global turnover, whichever is higher. Although authorities have so far not exceeded this penalty range, the level of company fines has increased significantly since the introduction of the GDPR in May 2018.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The collection and use of employees' personal data during internal investigations has to be in line with the GDPR and the Federal Data Protection Act; this applies in particular to email and data reviews as well as interviews. For each investigative step involving the processing of personal data, one must assess whether the processing is necessary for the purposes of the legitimate interests pursued by the company and whether the company's interests are overridden by the interests or rights of the respective data subject. Specific requirements apply with regard to employees when the private use of company information technology is allowed. Furthermore, affected employees must be informed about the subject and purpose of the investigation, and their rights under the applicable data protection laws, unless doing so would interfere with the integrity of the internal investigation. The involvement of entities other than the employing entity typically requires the conclusion of data protection agreements. Works council agreements (concluded to comply with German labour law) can stipulate further requirements.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The live monitoring of employees' communications is not explicitly prohibited under German data protection or criminal and labour laws, but the threshold for justifying measures of this kind is high and requires, inter alia, a thorough weighing of the company's interests – including the possibility of less invasive measures – against the rights and interests of the respective employee.

The review of historic email and other communication data is generally permitted if justified by legitimate interests of the company and if there are no overriding interests of the respective employee. To preserve proportionality, some specific rules for data reviews have to be observed, such as the exclusion of private data, search term filters and independent reviewers obliged to maintain secrecy. The employee's prior consent would only justify the processing of the data if it is given freely on an informed basis, which can generally be disputed in hierarchical structures.

© Law Business Research 2021

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In the course of criminal or cartel proceedings, companies are often subject to search and seizure measures. The relevant orders must, inter alia, include the facts giving rise to the suspicion and be proportionate.

Affected companies can, among other remedies, apply for a judicial review of such a measure or defend themselves against it by means of a judicial complaint. In practice, however, these legal remedies are mostly unsuccessful.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The conditions under which documents are exempt from seizure during internal investigations in Germany are largely unclear. To protect (potentially) privileged documents, the following measures, among others, may be taken:

- enter into an attorney–client relationship with the company affected by an investigation (and not, for example, its holding company) and document that the purpose of the mandate is (at least) to defend the company;
- do not establish a client's possession of work products at risk of seizure;
- take organisational measures to separate documents that are expected to be seizable from documents that are expected to be privileged; and
- label correspondence and documents as 'privileged' or similar.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Defendants have the right to remain silent towards the authorities and do not need to participate actively in the investigation (i.e., the right not to incriminate oneself).

Witnesses (at least in public prosecutors' offices and courts) are obliged, in principle, to provide information. As an exception, they may refuse to testify if (1) they are related to the defendant or (2) their testimony would expose them or a relative to the risk of prosecution.

If the witness is subject to the obligation of professional secrecy (as are lawyers), testifying may be refused in this regard.

© Law Business Research 2021

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is currently no general legal framework for whistleblowing in Germany. The EU Whistleblower Protection Directive (Directive (EU) 2019/1937) came into force in December 2019. EU Member States have two years from then to implement laws aimed at strengthening whistleblower protection in line with the Directive. From that point, at least larger companies will have a duty to implement whistleblowing systems. Whistleblowers who act in good faith will be protected from any retaliation if they report misconduct to the company or the competent authority. So far, the German legislature has not yet passed the implementing legislation.

Until the implementing legislation has been passed, German law provides protection for whistleblowers under general labour law principles and some specific provisions, such as with respect to the reporting of safety-at-work issues and prohibited uncovered short sales.

Currently, there is no general duty on German companies to implement whistleblowing structures under German law except for financial institutions (German Banking Act, Section 25a).

Financial incentive schemes for whistleblowers are not common in Germany and are not expected to be implemented in the near future. However, if the whistleblower is one of the perpetrators, disclosure to the authorities may well reduce a potential sentence significantly (see German Criminal Code, Section 46b). In cartel cases, the fine to be imposed on a cartel participant is even waived if he or she is the first to contact the German cartel authorities to uncover the cartel.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees are generally obliged to co-operate with internal investigations and no distinction is made between employees who are suspected of having committed a wrongdoing and those who have potential knowledge about a wrongdoing or just the circumstances surrounding it. Employees are obliged to co-operate even if their co-operation could result in them being convicted for specific crimes.

If an employee co-operates with an internal investigation, the company may have to cover the costs of the employee's legal counsel, subject to analysis in each case.

German data protection laws impose specific information duties on employers that process employees' information in the course of an internal investigation. Affected employees must be informed about the subject and purpose of the investigation and their rights under the applicable data protection laws unless doing so would interfere with the integrity of the internal investigation.

The duty to co-operate applies in the same way whether the individual is an employee, an officer or a director. However, directors are obliged not only to co-operate with internal investigations but also actively to initiate and conduct them.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Although there is no general differentiation between employees under suspicion and others, German labour and data protection laws require the weighing of an employee's interests against those of the company before measures are taken that affect the employee's rights. The degree of suspicion against an employee may tip the scales in this context.

Under German corporate law, a company's management board must investigate potential misconduct and put a stop to any misconduct discovered, revise the compliance programme and the internal controls affected and take steps, including concerning personnel, as a result of the misconduct. Therefore, the management board may be required to transfer certain employees or even give certain employees their notice, based on a thorough analysis in each case.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

In general, employees are obliged to co-operate with internal investigations, even if this could incriminate them. Depending on the specific case and the impact of the refusal, an employee may be dismissed for refusing to co-operate.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Yes, an investigation plan is key to an efficient and successful investigation. An investigation plan would normally include the scope of the investigation, the respective responsibility of the company and the law firm, the steps to be taken, the data and documents to be collected and the custodians.

The investigation plan is an important starting point and requires continuing revision subject to the findings made and the obstacles encountered.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

The concrete steps to be taken in this situation depend on the nature of the issue discovered. Generally, German corporate law imposes certain duties on a company's management board if there are indications of misconduct. First, the management board has to investigate the potential misconduct and put a stop to it. Second, the management board

© Law Business Research 2021

has to revise the compliance programme and the internal controls affected and take action, potentially including in respect of personnel, as a result of the misconduct.

To a certain extent, the management board can delegate these obligations to internal departments (e.g., compliance). However, to fulfil the board's supervisory duty, regular reporting to the management board of incidents handled by the internal departments is required. If an issue comes to light that points to severe misconduct or a matter that is potentially of high risk for the company, the management board should be notified immediately.

Although there is no general duty to report misconduct to the competent authority, reporting may be required in some specific cases. In particular, misconduct with a tax implication for the company has to be reported to the tax authorities in the vast majority of cases.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

First, it is generally advisable to enforce a litigation hold and to collect the respective data. This step should be extended to documents and data in the relevant context and should not be restricted to the documents and data requested by the law enforcement authority.

As a second step, the company will have to assess whether it is obliged to produce the requested data and documents. Independently of the result of this assessment, the company will have to answer the question of whether it is willing to co-operate and will have to find a strategic position regarding the authority. In many cases, it is advisable to co-operate with the enforcement authority to prevent coercive measures and reputational damage.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

In general, there is no duty to publicly disclose the existence of an internal investigation or contact from a law enforcement authority. Whether a disclosure is made or not largely depends on the interests of the company in the specific case.

Exceptionally, stock listed companies may be subject to a disclosure requirement if the investigation has an effect on the company that would be likely to significantly affect the company's stock price (ad hoc announcements).

37 How are internal investigations viewed by local enforcement bodies in your country?

Especially in larger and complex proceedings, authorities welcome internal investigations as part of a company's pledge to co-operate with a criminal investigation. In our experience, in most cases, authorities take into account the costs of an internal investigation when it comes to sanctions and fines if the internal investigation is done properly and the company has co-operated fully with the authority.

As far as possible, the measures to be taken as part of an internal investigation conducted in parallel with an official investigation should be coordinated with the authorities.

© Law Business Research 2021

Otherwise, there is a risk that an authority might feel obstructed by an internal investigation and that a possible bonus could turn into a handicap.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

German case law is inconsistent on this issue. In principle, protection against seizure depends on whether (1) the company is already under an official investigation or at least objectively likely to be officially investigated and (2) the relevant documents are drafted for defence purposes.

To protect potentially privileged materials, a company may adopt protective measures, such as to:

- enter into an attorney–client relationship and document that the purpose of the mandate is (at least) to defend the company;
- not establishing possession of work products at risk of seizure;
- take organisational measures to separate documents that are expected to be seizable from documents that are expected to be privileged; and
- label correspondence and documents as 'privileged' or similar.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

German case law is inconsistent on this issue. In principle, protection against seizure depends on whether (1) the company is already under an official investigation or at least objectively likely to be officially investigated and (2) the relevant documents are drafted for defence purposes. In general, these principles apply to both companies and individuals.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The protection from seizure applies in principle only to defence communication with external counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Protection from seizure can also cover the work-product of foreign lawyers drafted in their capacity as defence counsel. International attorneys, however, may be subject to restrictions as to their ability to appear in court.

© Law Business Research 2021

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The disclosure of privileged documents is generally regarded as a co-operative step by national authorities. However, there is no general concept of waiving privilege under German law.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no concept of limited waiver of privilege in Germany.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Waiving privilege in another country has no direct legal effect on privilege claims in Germany. However, it is possible that the waived documents may be seized from the third person abroad if he or she does not enjoy protection against seizure under German law.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privilege does not exist in Germany.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

The question as to the extent to which assistance should also be included in protection against seizure has not yet been conclusively clarified by case law. As a rule, the further documents leave the sphere of an external counsel, the weaker their protection.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Interviews are an important and common part of internal investigations in Germany.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

National case law is inconsistent on this issue. In principle, protection against seizure depends on whether (1) the company is already subject to an official investigation or at least objectively likely to be officially investigated, and (2) the relevant documents are drafted for defence purposes.

In respect of interview protocols and attorney reports, it should be argued that these work-products also serve as preparation for corporate defence and are therefore privileged.

© Law Business Research 2021

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

An employee is generally obliged to co-operate with internal investigations and to tell the truth even at the risk of self-incrimination. This may not apply to interviews of third parties, such as former employees.

As many employees are not aware of their duty to tell the truth, it is customary to inform them about it in an introduction. Other customary elements of the introduction, if applicable, are as follows:

- notification that the legal counsels conducting the interview are the company's lawyers and are not acting for the interviewee;
- the possibility of an employee engaging his or her own attorney and clarification about the costs. If relevant and to prevent disruption, this information may be provided in the invitation to the interview;
- the company may choose to share part of or all information provided in the interview with national or foreign courts or law enforcement authorities;
- refusing to co-operate may lead to disciplinary action;
- the modus of the protocol, whether the employee will be granted access to it and whether he or she will have to confirm its content; and
- the employee's data protection rights, ideally accompanied by this information in writing.

Essentially, this information is very similar to the *Upjohn* warning concept developed in the United States.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

An interview usually begins with a briefing about, inter alia, the subject of the interview and the interviewee's rights. The interview environment should be appropriate (e.g., a neutral meeting room on the company's premises or the law firm's offices) and – depending on the duration of the interview – sufficient breaks, drinks and food should be offered.

Depending on the stage of the internal investigation, documents may well be shown to witnesses during interviews.

German case law is not yet settled on the question of whether an employee has the right to be accompanied at an interview by his or her own counsel and who has to bear the costs. However, companies usually allow interviewees to have a legal representative of their own in attendance, at least when the company is represented as well. In the recent past, there have been discussions as to whether an employee's right against self-incrimination in internal investigations shall be introduced into German law.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

In principle, there is no obligation in Germany to report misconduct to law enforcement authorities. Exceptionally, however, individual statutory regulations may require a report. This applies, inter alia, in connection with incorrect tax returns and the field of money laundering.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

This depends on a comprehensive analysis in each particular case. Generally, if there is a high risk that the competent authorities may get hold of the information or the company's future business may be compromised as a consequence of the undisclosed misconduct (e.g., if a declaration of honour cannot be signed), disclosure may be advisable.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

First, you should make sure you have the right timing, in particular with respect to the ongoing investigations. Then, the company representative should contact the competent authority and set up a meeting for initial discussions based on a summarised set of facts, including evidence. During this meeting, there should be mutual agreement about any further proceedings.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

This will depend on the status of the investigation and the negotiations. It is generally possible to discuss requests made by the authorities. It is important to understand that, although there is no legal duty to reply to requests for information in criminal investigations, refusal to do so is likely to lead to a raid by the law enforcement authority.

55 Are ongoing authority investigations subject to challenge before the courts?

The investigation itself cannot be challenged in court.

© Law Business Research 2021

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Preventing inconsistent communication with different authorities is certainly important. However, it should be considered that in particular in complex investigations, different authorities develop different focus areas, for example as a result of a different legal assessment.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In principle, companies are not obliged legally to produce any material from abroad. However, refusal to do so could lead to legal assistance requests from German authorities to their foreign counterparts and would be seen as unco-operative, thus jeopardising any co-operation bonus. Therefore, it might be advisable to produce documents that are outside Germany, provided the company has the power to do so under company law. In these situations, the company is also obliged to respect local laws, in particular data protection laws.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Law enforcement authorities have implemented cross-border communication networks and coordination units to co-operate effectively, and we have seen a rise in the scale of international co-operation. The legal framework is fragmented and includes EU regulations as well as bilateral and multilateral treaties.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Generally, investigating officers are bound by confidentiality with respect to information received in the course of an investigation. However, third parties may have a right to access the investigation file or parts of it, for instance, to prepare civil claims against the perpetrator.

Public officials in the tax authorities are additionally obliged to observe tax secrecy (under the German Fiscal Code, Section 30).

© Law Business Research 2021

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Subject to a thorough assessment of the local law prohibiting the production, we would generally advise complying with applicable law and trying to convince the German authority either to forego the requested documents or to seek administrative co-operation to formally seize the documents locally.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Both the European Union and Germany have introduced certain blocking statutes. A violation of either national or EU blocking legislation is punishable by law and may result in severe fines. We would generally advise engaging with the investigating authorities to evaluate alternatives.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Before voluntarily producing documents, privilege issues in cross-border situations have to be considered. In addition, in the case of voluntary production, increased attention should be paid to aspects of data protection. With respect to confidentiality, there are no relevant distinctions between voluntary production and compelled production under German law.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Individuals can be sanctioned by fines or imprisonment. They may also be banned from carrying on their profession.

For companies, fines and profit confiscation are particularly relevant. In addition, exclusion from (public) tenders can have a significant negative effect.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

A debarment under German public procurement law can also be based on misconduct by the company or its employees abroad. To mitigate this risk, a settlement abroad should be accompanied by self-evaluation and remediation measures by the company in Germany. These actions may include disciplinary measures against the individuals

© Law Business Research 2021

involved, compensation for damage sustained, co-operation with investigating authorities and strengthening of the compliance management system.

65 What do the authorities in your country take into account when fixing penalties?

Authorities take into account, inter alia, the degree and extent of the misconduct committed, the subjective accusability of the misconduct, economic circumstances and the extent to which the parties concerned have co-operated with the investigating authorities. In addition, the Federal Supreme Court has ruled that the design of a compliance management system and the extent to which it was adapted at the time of the misconduct, and the improvements implemented after the misconduct, must also be taken into account.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Not at the moment. Currently, settlements with authorities are reached via a 'negotiated' fine or confiscation order in which the misconduct and the facts are described. Under German law, neither the order nor the statement of facts is made public. Nevertheless, in high-profile cases, the authorities usually issue a short press release summarising the facts of the case (approximately one to two pages). The settlement needs no approval by the court but lies in the discretion of the public prosecutor. German authorities often expect the company under investigation to improve their internal structures before a settlement is made to achieve a decent deal.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies should consider in particular the economic and reputational effects of the settlement itself, the (regularly positive) consequences of terminated investigations for the operational capacities of the company, the consequences for public procurements (e.g., potential debarments in Germany or abroad), further co-operation with investigations against individuals and the structural consequences to be drawn to prevent similar misconduct in the future.

© Law Business Research 2021

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Corporate compliance monitors are not currently foreseen by the law and are therefore not used in Germany.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel private actions are allowed. In some cases, however, civil courts tend to suspend proceedings until criminal proceedings on the same subject have been completed.

Private plaintiffs may have the right to access criminal files if, inter alia, they present a legitimate interest in this and if this is not opposed by the overriding interests of the defendant or other persons who are worthy of protection.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In principle, investigations are not public. However, they regularly become publicly known if the case is interesting enough. Apart from a few exceptions, criminal trials are public.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

This depends on the specifics of the case and the in-house capabilities of the company. In larger-scale cases in which public opinion is of greater relevance, the engagement of public relations consultants is quite common. The communication strategy needs to be fully aligned with the company's internal findings and legal defence strategy. In our experience, the communication strategy should strike a balance between 'litigation language' and frank and honest communication.

73 How is publicity managed when there are ongoing related proceedings?

Usually, no substantial public statements on the allegations should be made while the facts are still under investigation. If possible, next steps can be communicated.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

This must be assessed in each particular case, taking into account all rights and legitimate interests of the company, its shareholders and the authorities involved.

© Law Business Research 2021

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

ESG-related matters have gained prominence in German legislation in the past few years. It would go beyond the scope of this publication to list them all. Therefore, we focus on the main regulations on ESG.

Non-financial reporting

In accordance with Directive 2014/95/EU (the Corporate Sustainability Reporting Directive), Germany has established several non-financial reporting duties for listed companies with total assets of more than €6 million or an annual turnover of more than €12 million, and financial institutions and insurance companies with more than 500 employees in their annual report. The annual report shall outline the main risks that exist with regard to labour, social and environmental issues. Further, it shall state which concepts the company employs to combat these issues as well as the measures undertaken with regard to respecting human rights and to prevent corruption. If the company does not adopt a concept regarding these matters, it needs to explain why this is the case ('comply or explain'). Companies that do not incorporate such a non-financial report in their annual report are at risk of incurring a fine.

Further, Regulation (EU) 2019/2088 on sustainability-related disclosures in the financial services sector affects financial market participants (e.g., investment firms and banks offering portfolio management) as well as financial advisers (e.g., a credit institution or an investment firm that provides investment advice). It requires the publication of sustainability-related information at both the company and the product levels.

Transparency at the company level includes, inter alia, disclosure on the company website of, among other things, strategies for the inclusion of sustainability risks and information about the material adverse effects on sustainability factors and explanations of the remuneration policy, including a description of how it is consistent with the inclusion of sustainability risks.

If financial products are advertised or offered with environmental or social characteristics or as sustainable investments, the following must be complied with:

- extensive pre-contractual information, including information about investment strategies, intended investment goals, the expected effects of sustainability risks on the return, indices used as reference values, etc.;
- comprehensive product description on the website of the financial market participant; and
- detailed explanations in the regular reports by the financial market participant, including the extent to which the features or the investment goals have been met.

Sustainability

Sustainability factors gain more and more prominence in public procurement law since the legislator decided that these factors can also be taken into account when awarding public contracts.

© Law Business Research 2021

Equal participation in corporate leadership

In August 2021, the legislator amended the Stock Corporation Act with the Act on the Equal Participation of Women in Leadership Positions. Under this Act, the board of directors of any listed company that is subject to the Co-determination Act must include at least one woman or one man if the board consists of more than three persons, among other things.

Corporate responsibility in supply chains

The legislator has implemented the Act on Corporate Responsibility in Supply Chains, which has been influenced by the UK Slavery Act to a certain extent. As of 1 January 2023, it requires corporations that are headquartered in Germany and employ more than 3,000 people group-wide in Germany and abroad, or have a branch in Germany and employ more than 3,000 people in Germany (these numbers will be reduced to 1,000 employees as of 2024), to adhere to human rights and environmental standards in their supply chains. The term 'supply chain' encompasses all stages of production, domestically or abroad, irrespective of whether the process takes place within the company or with a supplier, which is necessary to manufacture the company's products or provide its services.

The duties under the Act include, inter alia:

- the establishment of a risk management system that entails frequent risk analyses;
- the definition of the responsible internal unit;
- the issuance of a declaration of compliance;
- the establishment of prevention measures within the company and in respect of suppliers;
- remedial actions in the event of a violation of human rights or environmental standards; and
- the establishment of a grievance procedure.

Compliance with the duties under the Act needs to be documented regularly. Additionally, companies shall prepare an annual report of its compliance with the duties under the Act during the previous business year and make the report available to the public on the company's website for seven years.

In the event of a breach of one of the duties under the Act on Corporate Responsibility in Supply Chains, the government can exclude companies from public tenders. Further, companies may risk a fine of up to €800,000 or up to 2 per cent of the annual global group turnover if it exceeds the threshold of €400 million. The competent management can be sanctioned individually with a fine of up to €800,000.

German Corporate Governance Codex and ESG

Since 2019, the German Corporate Governance Code, with which listed companies have to adhere on a comply or explain basis, states in its foreword that with its actions, the company and its governing bodies must be aware of the enterprise's role in the community and its responsibility towards society. Social and environmental factors influence the enterprise's success. In the enterprise's best interests, the management board and

© Law Business Research 2021

supervisory board should ensure that the potential effects of these factors on corporate strategy and operating decisions is identified and addressed.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Owing to the federal elections in September 2021, it is hard to estimate which legislative projects will be introduced by the new government in the coming year. However, one potential law could be the Whistleblower Protection Act, which implements the EU Whistleblower Protection Directive.

The election programmes of the three major parties in Germany contain vague proposals for legislative projects relating to ESG matters. In general, they agree that environmental issues should be on the agenda. It remains to be seen whether this will lead to stricter regulations for companies.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

In recent years, ESG-related litigation has gained some prominence in Germany. Although most of the cases are still brought up against the government, we know of several lawsuits that have been filed against companies. We expect that ESG-related litigation will continue to gain importance in the near future, especially as a result of new legislation (such as the Act on Corporate Responsibility in Supply Chains).

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Owing to the federal elections in September 2021, a legislative change in the coming year seems unlikely. Overall, it remains to be seen whether a bill on corporate criminal liability will be taken up again under a new government.

© Law Business Research 2021

13

Greece

Ilias Anagnostopoulos, Jerina Zapanti and Alexandros Tsagkalidis[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Based on the findings of a financial investigation conducted by third parties, it was revealed that, from 2001 to 2017, the management of a Greek-based international company that designs, manufactures and distributes luxury jewellery and watches had falsified its financial statements by inflating its sales, profits and equity through virtual purchases and sales. These fictitious transactions allegedly took place between 27 companies in different parts of the world, mainly in Asia. After the conclusion of a preliminary inquiry and a formal investigation, the Indicting Chamber with the Court of Athens decided on the indictment of the former chief executive officer and other defendants, including the founder of the company, on the charges of forming a criminal organisation, falsifying the company's financial statements, market abuse, money laundering and embezzlement.

Other major investigations have been conducted in relation to multinational companies that have reportedly been systematically giving money to public officials to secure awards of multimillion-euro government contracts in respect of advanced communication systems, medical supplies and military expenditure (such as Siemens, Johnson & Johnson/DePuy, HDW/Ferrostaal and STN). Investigations have also targeted acts of corruption of former government officials in relation to facilitating payments and tax fraud schemes through real estate deals.

1 Ilias Anagnostopoulos, Jerina Zapanti and Alexandros Tsagkalidis are members of Anagnostopoulos.

© Law Business Research 2021

2 Outline the legal framework for corporate liability in your country.

Criminal liability is an exception when referring to a legal entity because, under Greek law, only an individual may be liable for a criminal act. However, harmonisation with international corporate standards, and the need to bring internal legislation in line with European and international instruments, has led to provisions for liability of entities in the form of administrative measures and fines, among other things.

Corporate conduct may be punishable in certain cases. Company conduct (e.g., in the context of anti-corruption, anti-money laundering and anti-cartel legislation) is usually punishable when it is linked with positive gains or advantages. The company is liable as an entity – notwithstanding the individual liability of employees – when there is some type of profit, gain or advantage to the company. The severity of punishment in these cases (in the form of administrative penalties or fines) usually depends on the type of profit or gain, and the annual turnover of the company.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The responsibility for the investigation of corporate conduct lies with regulatory and prosecuting authorities (depending on the scope of the investigation) but the responsibility for criminal prosecution of corporate conduct always lies with the Prosecutor's Office. Regulatory authorities may investigate – within their scope – corporate conduct (e.g., the Competition Commission for cartel offences or the Capital Market Commission for insider dealing or market abuse), and any findings relating to criminal offences are forwarded to the Prosecutor's Office to decide on further proceedings.

It is most common for the Economic and Financial Crime Unit (SDOE) to undertake the necessary preliminary investigations, evidence gathering, reports and so on, following a prosecutorial order. In cases of money laundering, the Greek Financial Intelligence Unit gathers all necessary information and evidence, and if it believes there is enough to support a criminal case, it forwards the case to the Prosecutor's Office.

The Prosecutor's Office opens a case against the natural person or officers of an entity, following standard criminal procedure, namely conducting a preliminary investigation, filing charges and making a referral to investigation (conducted by an investigating judge). It is not unusual in serious and complex cases (e.g., corruption, large-scale money laundering and fraud) for enforcement agencies and the Prosecutor's Office to take action to secure evidence (by issuing either a warrant for search and seizure or a freezing order) before any charges are filed and before persons of interest are called for questioning.

Companies are not criminally prosecuted because they are not criminally liable, but sanctions are imposed against them in the form of administrative penalties for the actions of individuals held liable for criminal acts from which the companies have benefited.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

A preliminary investigation is initiated by the Prosecutor's Office following a *notitia criminis*, namely a criminal complaint (by an individual or entity, usually the victim of

© Law Business Research 2021

a crime) against certain persons, or information submitted to the Prosecutor's Office by another authority, or even information that has come to the knowledge of the Prosecutor's Office through the media or any other sources, and it is usually the very first stage of the proceedings. It is ordered by a prosecutor, unless an agency or enforcement authority may by law gather evidence and information through a preliminary enquiry and submit a request to the Prosecutor's Office for further investigation. All preliminary investigations, apart from regular tax reviews, are supervised by the Prosecutor's Office.

The standard of proof to open a preliminary investigation is low. Even slim evidence of an alleged criminal offence (e.g., unconfirmed press reports or anonymous information) may justify a preliminary investigation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The prosecutor or the investigating judge who supervises the investigation should be informed regarding any objections raised against a notice or subpoena. Also, if there is a disagreement between a defendant and the prosecutor or the investigating judge regarding such matters, the validity or lawfulness of a notice or subpoena could be challenged before the Judicial Council, according to the provisions of the Code of Criminal Procedure.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Yes. Articles 263A and 187C of the Criminal Code (CC) provide for immunity or leniency for individuals who inform or assist (or both) the prosecuting authorities in corruption cases (263A) or cases involving criminal or terrorist organisations (187C).

7 What are the top priorities for your country's law enforcement authorities?

The detection and prosecution of corruption is one of the main goals of prosecuting and enforcement authorities. Legal provisions in respect of acts of corruption were amended three times between 2014 and 2019 to conform with international instruments. Greece has ratified all major EU and international conventions and has passed internal legislation to comply with them. However, continuous amendment of existing legislation creates legal uncertainty and poses complex issues in respect of pending investigations or ongoing trial hearings. More generally, it is apparent that an integrated anti-corruption policy is needed, including better coordination of various legal instruments and anti-corruption agencies.

© Law Business Research 2021

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

The CC, in Article 236 paragraph 3 (bribery of a public official) and Article 237 paragraph 3 (bribery of a member of the judiciary), stipulates that a director of a corporation who negligently failed to prevent the commission of the stated bribery offences by an employee of the corporation is punishable by imprisonment for up to five years and a monetary penalty. Therefore, not having an effective compliance programme in place will be deemed an illegal act punishable by the above-mentioned statutes if an act of bribery for the benefit of the company is committed by that company's employees.

Moreover, Law 4706/2020 on Corporate Governance and Capital Market Modernisation (published 17 July 2020) stipulates that a corporation is obliged to have an effective compliance programme in place as part of its Regulation of Internal Operations. Guidance is provided by the regulating bodies of each sector (such as the Bank of Greece), which issue by-laws stating the minimum requirements of compliance.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

In 2016, Greece transposed Directive 2013/40/EU on attacks against information systems, replacing Council Framework Decision 2005/222/JHA, and amended its criminal legislation accordingly to strengthen cybersecurity protection; in particular, under the Criminal Code (CC), to punish:

- hindering the operation of information systems (Article 292B);
- the supply of hardware or software for the purpose of hindering the operation of information systems (Article 292C);
- unlawful access to an information system (Article 370C);
- unlawful extraction of data from an information system (Article 370D); and
- computer fraud (Article 386A)

The investigation of criminal cases in relation to the above-mentioned crimes is handled by the Cyber Crime Division of the Hellenic Police. After its investigation is finished, it forwards the case file to the prosecutors with the court of first instance.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

All regular crimes committed with the use of a computer are punished by Greek law. Special provisions can be found for the crimes of child pornography and attracting children for sexual purposes through information systems (CC, Articles 348A and 348B). The Cyber Crime Division of the Hellenic Police also handles the investigation of cybercrimes.

© Law Business Research 2021

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

As a general rule, Greek law does not have extraterritorial effect. Enforcement and sanctions imposed by the Greek authorities are not effective in other jurisdictions unless they meet the requirements of mutual assistance in criminal matters and mutual recognition of judgments through bilateral and multilateral treaties.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations and co-operation with other countries' law enforcement or prosecutorial authorities have become common practice in large-scale investigations. Special law enforcement agencies, such as the Economic and Financial Crime Unit, have entered into agreements with similar agencies in other countries, which has enabled a faster and more efficient exchange of information. Agreements between agencies usually follow framework agreements or treaties between countries. In the case of Greece, most aspects of international co-operation are treaty-based. There are two sets of rules applicable to this prosecutorial co-operation, one of which applies to co-operation with Member States of the European Union (in these cases, all procedures and functions are simplified and faster). In all other cases, provisions for mutual assistance apply (for investigating acts or requests for information).

Greek legislation has undergone a series of amendments to fully comply with international treaties and the obligations arising from Greece's participation in international organisations, among others. However, the introduction of new legislation and measures not totally compatible with existing procedures and practices has prevented a smooth integration of new measures with traditional prosecutorial and investigative practices. Also, efforts to adjust legislation to international instruments as much as possible (especially in combating corruption and money laundering) have led, in many instances, to the powers of different law enforcement agencies overlapping, and there is no general rule or central authority to resolve such issues or to propose any necessary adjustments.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The rules on double jeopardy, or *ne bis in idem*, are not directly applicable to entities as they are not the subject of a criminal prosecution. These rules may be applied indirectly (through examination of individual criminal liability) but this is a disputed matter.

© Law Business Research 2021

14 Are 'global' settlements common in your country? What are the practical considerations?

No. In certain cases, Greece has entered into a settlement in the context of ad hoc agreements with the companies under investigation. These types of settlements do not cover the criminal liability of individuals, such as directors or employees of the company.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Foreign decisions are usually taken into account by Greek courts in relation to the findings regarding the merits of the case, but they do not bar Greek proceedings from advancing. The Greek state, in practice, applies its law to companies for conduct within the country or for acts that have effects within the country. In this respect, Greek authorities seek to impose the law on companies either registered in Greece or active in the Greek economy (e.g., companies with registered offices in other countries that have agencies or subsidiaries in Greece).

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Greece does not have its own sanctions programme but sanctions are imposed through EU Regulations, which are directly applicable, and by UN Resolutions, which are implemented by Presidential Decrees.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Greece does not have its own sanctions programme. Information regarding sanctions enforcement can be found through the EU sanctions map, which is published online.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

As regards the freezing and unfreezing of assets of states, legal persons, legal entities or natural persons imposed by UN Security Council resolutions, UN decisions or pursuant to EU Regulations or Decisions, for any legitimate reason under international law, the competent authority is Unit B of the Hellenic Financial Intelligence Unit. As regards restrictions on imports and exports, the competent authority is the General Directorate of International Economic Policy, Directorate of Import-Export Regimes and Trade Instruments of the Ministry of Development and Competitiveness. These authorities often liaise, coordinate and communicate with their foreign counterparts to exchange information.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Council Regulation (EC) No. 2271/96 (known as the EU Blocking Regulation) is directly applicable in Greece.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Regarding the freezing and unfreezing of assets of states, legal persons, legal entities or natural persons, Unit B of the Hellenic Financial Intelligence Unit, which is also known as the Financial Sanctions Unit, is responsible for enforcing such sanctions. The General Directorate of International Economic Policy of the Ministry of Development and Competitiveness has powers to enforce restrictions on imports and exports to specific countries. All sanctions are based on UN Security Council Resolutions, UN Decisions, or EU Regulations or Decisions.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of corporate misconduct most often come to light through investigations conducted by regulatory agencies such as the Competition Commission, the Capital Market Commission and the Financial Intelligence Unit in respect of breaches of regulations within their competence. The authorities regularly receive related information (officially and unofficially) from a number of sources, including whistleblowers. Self-reporting by companies is still rather unusual.

INFORMATION GATHERING

22 Does your country have a data protection regime?

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation) came into effect in May 2018. Legislation is currently being drafted to implement the Regulation.
- Law 4624/2019: Hellenic Data Protection Authority (HDPA), measures for implementing the General Data Protection Regulation.
- Law 2472/1997: Protection of Individuals with regard to the Processing of Personal Data.
- Law 3471/2006: Protection of personal data and privacy in the electronic telecommunications sector and amendment of Law 2472/1997.
- By-laws issued by the HDPA.

© Law Business Research 2021

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The HDPA is a constitutionally independent administrative authority that supervises the application of data protection laws and regulations, and imposes administrative sanctions on natural or legal persons who violate those laws. The primary mission of the HDPA is the protection of individuals from the unlawful processing of their personal data and providing assistance if it is established that an individual's rights have been violated in any sector (such as financial, health, insurance, education, public administration, transport or mass media).

Moreover, criminal sanctions may be imposed by the courts on persons who violate data protection legislation.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Internal investigations are not regulated by special legal provisions, so the general rules concerning data protection and privileges apply. As a general rule, employees must be loyal to the company they serve, handle sensitive information with care and avoid activities that conflict with the company's interests. Nevertheless, the company, as an employer, must respect and protect sensitive personal information about its employees and any personal communications.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

It is common practice, also recognised by the Greek courts, for an employer to have access to its employees' business communications, such as emails, calls or text messages circulated through the company's communication infrastructure (servers, backup storage, etc.). In most cases, this type of access is provided for in the company's internal work regulations and is agreed by both parties in the employment contract.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In the majority of cases, the authorities will send a written request to a company to provide certain information or documents. In principle, a company must co-operate with the authorities, at least in terms of providing requested information and documentation. Failure to comply with such a request usually has no direct consequences (unless otherwise provided for by law) but may lead to an unfavourable report by the authorities or an on-site search and seizure to obtain requested material.

© Law Business Research 2021

In all cases, the company may object to handing over certain documents or material (e.g., privileged commercial information or correspondence) and refer to the Prosecutor's Office to resolve the issue. In practice, when an on-site search is in progress, the company may not refuse to hand over material but may raise its objections regarding the nature of the material taken (e.g., privileged information) when signing the confiscation documents, in which case the material is sealed and taken by the agency, pending resolution of the issue by the courts.

On some occasions (depending on the scope and nature of an investigation), the company may be requested to submit its views in respect of the issues under investigation or to offer evidence in its defence (of any type: witnesses, bank records, correspondence, and others) contesting the views of the investigating authority (usually included in a draft report).

Dawn raids may take place in emergency situations (to secure evidence, for instance) and home searches are conducted in the presence of a prosecutor or magistrate.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

According to Article 212 of the Code of Criminal Procedure (CCP), information in the possession of clerics, lawyers, doctors, pharmacists and military diplomatic officials is considered privileged. During a search of its premises, a company may declare that certain documents are privileged information pursuant to Article 212 of the CCP. If the investigating authority contests this assertion, it will confiscate the documents, seal them without acquiring knowledge of their content and request the competent professional association to decide on the confidentiality of the seized documents. The general rule is that documents containing privileged information may not be included in the confiscated documents. This restriction is not applicable when the person protected by privilege (such as a lawyer, doctor or cleric) is under investigation as an accomplice in a criminal act. Personal documents of employees are protected to a certain extent, depending on the specifics of the case.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

All authorities with the power to conduct investigations in their field (e.g., the Prosecutor's Office, the police, the Financial and Economic Crime Unit and the Capital Market Commission) may request that individuals give statements following an order by the Prosecutor's Office or in accordance with specific legal provisions. In cases of serious business crimes, the Prosecutor's Office usually orders a specific person to give a statement either as a witness or as a suspect (witness under caution) while the actual questioning is most commonly conducted by the police or the Financial and Economic Crime Unit (which is an agency supervised by the Ministry of Finance and has powers similar to the police, such as conducting investigations, examining witnesses and performing on-site inspections).

© Law Business Research 2021

If an individual is called as a witness, he or she appears before the authority that has received the Prosecutor's Office's order and gives a statement under oath. Persons called as witnesses to provide testimony must appear before the authority that conducts the investigation to answer questions. Witnesses have the right to avoid self-incrimination.

Individuals called as suspects have the right to request a copy of the case file and sufficient time to prepare for questioning. At this preliminary stage, suspects are also entitled to a defence attorney, who may be present during questioning, and to file written submissions in their defence.

In all cases where questioning of individuals as suspects is involved, relevant provisions of the CCP apply, namely the right to avoid self-incrimination, the right to an attorney, time to prepare one's defence, the right to remain silent, and so on. The structure of the pretrial procedure is such that a suspect may have full representation by a defence attorney and full protection of his or her rights.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Greece does not have systematic legislation protecting whistleblowers in either the public sector or the private sector, nor does it have any relevant financial incentive schemes. Whistleblowers may be considered as witnesses in the public interest, which results in complete protection from criminal prosecution with respect to offences such as disclosure of privileged information or filing a false complaint relating to the information the whistleblower provides to the authorities, according to Article 47 of the Code of Criminal Procedure.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Local employment law does not grant special rights to employees who are under investigation, nor does it distinguish between officers and directors. Nevertheless, employees must be treated with respect, and the investigation should be conducted in accordance with data protection and labour laws.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

In cases of alleged serious misconduct, both employees and directors are usually notified in case the individual wishes to have counsel present at interviews; it is for the individual to decide on the presence of counsel.

© Law Business Research 2021

A company's policy in cases of individual liability will depend on the type of misconduct (negligent or deliberate), the seriousness of the actions and the position of the individual, among other things. It is customary for a company to collaborate with an individual's counsel when the action occurred as a result of his or her position in the company (e.g., administrative proceedings or criminal proceedings against a managing director for an environmental offence).

Termination of an employee's contract is something about which the company has to decide after reviewing the whole case and assessing possible consequences for the entity. If the employee has acted against the company's best interests and the actions are the reason the government seeks to impose liability, the company may have no option but to terminate the contract to protect its interests, privileged information, and so on. In the end, it is a strategic decision for the company unless the particulars of the case leave no option other than to terminate the employment. This is especially the case when an employee is involved in large-scale or serious violations of duties, has deliberately acted against the company's interests, or engaged in fraudulent activity against the company itself, its clients or the general public.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

The obligation of an employee to participate in an internal investigation depends on the terms of the employment contract and the applicable law. Refusal to participate in internal proceedings could eventually lead to dismissal.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

No special statutory rules regulate internal investigations. Thus, the way in which internal investigations are conducted varies. Usually, the department of a company that is to conduct the investigation decides how to proceed.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no general rule or obligation for self-reporting. A series of legislative measures have been passed to enable enforcement agencies to detect misconduct with or without the co-operation of the companies. In this respect, accounting officers must report any suspicious activity (relating to tax evasion, money laundering and the like) if there are indications of misconduct.

However, there are special provisions in numerous laws and regulations that stipulate self-reporting of internal wrongdoing and cover most aspects of business activity. In some fields or industries, provisions for self-reporting are more stringent (e.g., banking and

© Law Business Research 2021

financial services), while in others there is no explicit provision for self-reporting (most commercial activities in the private sector); however, rules for reporting criminal acts to the authorities (as a general legal obligation) may apply and this might, to some extent, lead to some kind of self-reporting.

There are specific industries or fields in which self-reporting is a prerequisite to obtaining the benefit of leniency measures or for immunity provisions to apply in cases of violations of competition law, exposure of corrupt practices of public officials, organised crime and terrorism.

In any of these procedures, the authorities can choose to impose lesser penalties or grant complete immunity. These provisions may apply to corporate entities only, to individuals only, or to entities and individuals alike. Considering that, in the majority of cases involving serious corporate misconduct, the authorities may impose administrative penalties and measures affecting the company's ability to continue and develop its activities, as a rule, participation in a leniency programme is considered the better option for a company and the implicated individuals.

Where leniency or immunity measures are provided for (e.g., cartel offences, corrupt practices or money laundering), the extent to which they apply depends on the type of information provided to the authorities. As a rule, effective and complete exposure of illegal practices may lead to lesser penalties or immunity from criminal prosecution or administrative sanctions. Immunity would usually be granted when the reporting of illegal practices is of such significance that it contributes substantially to the exposure of illegal activity or perpetrators.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

- Notify the legal department regarding the nature of the notice or subpoena and consult on how to proceed next.
- Retrieve any requested documents or data.
- Evaluate the possible implications from a criminal and an administrative perspective in relation to the requested documents or data.
- Decide whether and how to comply with the request.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

No general obligation is provided for by Greek law, but in certain fields (e.g., competition regulation), corporations are given motives for self-reporting through provisions for leniency or immunity programmes, or both. Listed companies must disclose relevant information to the public in accordance with the existing regulations.

© Law Business Research 2021

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are welcomed by the law authorities, when they are conducted in a manner that leads to direct gathering of evidence, preservation and referral of evidence to the authorities. However, the absence of a clear legal framework for regulating internal investigations poses complex issues in relation to the protection of affected individuals.

ATTORNEY-CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

The attorney–client privilege may be asserted at any time. However, it is not always easy to determine what falls under this protection. Apart from the obvious privileged information (such as correspondence between an attorney and a client), there are other forms of communication (e.g., memos, drafts of letters or other documented material) that may contain privileged information.

The company is not expected to waive its rights or privileges (especially the attorney–client privilege) as part of its co-operation with the authorities. However, the company may choose to waive its rights in whole or in part with respect to such privileges if it becomes necessary for the purposes of its defence in regulatory or criminal procedures. For documents and material protected by special legislation (e.g., patents), the company is entitled to deny access, give limited access or request that the material be handled by the competent authorities in accordance with special legal provisions.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The attorney–client privilege is considered to be of paramount importance and is well established in Greek legislation. Sources of this privilege are to be found in the Lawyer's Code of Conduct, the Code of Criminal Procedure, the Criminal Code and the Code of Civil Procedure. The attorney–client privilege is broad and covers any type of data (verbal, written, electronic, etc.) obtained from the client, regardless of whether the client is a natural or a legal person. The attorney–client privilege may be invoked even after the termination of the relationship between an attorney and a client.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes. In Greek law there is no distinction between in-house and external counsel in this respect.

© Law Business Research 2021

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

No. In principle, it applies to lawyers registered in Greece.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiving the attorney–client privilege is not common practice in the legal system and is not provided for as a mandatory or required step in any context.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

When a company is requested by the authorities to produce privileged information (and has decided to comply with the request), it is common practice to provide limited information relating only to the scope of the request. However, no effective safeguards are in place as to how the information provided could be used by third parties, including other authorities and agencies.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Yes. Waiver of privilege is valid only when it is conducted according to the provisions of Greek law.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

There is no special rule regarding common interest privilege. It falls under the attorney–client privilege.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

There is no explicit legal provision or relevant case law covering this matter. Privilege can be claimed regarding the documents in the lawyer's possession. However, it is doubtful whether privilege would apply to communications between lawyers and third parties or in relation to documents in the possession of third parties.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

© Law Business Research 2021

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Currently there is no clear legal framework for regulating internal investigations. Therefore, witness interviews of employees must be conducted with respect and in accordance with data protection and labour laws. It should be noted that the obligation of an employee to be examined as a witness in the course of an internal investigation depends on the terms of the employment contract and the applicable law. Refusal to participate in internal proceedings could eventually lead to dismissal.

Third parties are not obliged to testify as witnesses in corporate internal proceedings.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no established protocol for conducting internal interviews of witnesses. It is usually decided by the department within the company that is to conduct the investigation, which also decides on the strategy of the questioning and whether documents will be put to the witnesses. In cases of alleged serious misconduct, the employee is usually notified in case he or she wishes to have counsel present; it is for the employee to decide about the presence of counsel.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

A business may conduct its own internal investigation on any occasion. Whether the results should be shared with the authorities depends on the results and the nature of the case, since there is no general rule for self-reporting – with the exception of certain aspects of business activities usually relating to regulatory rather than criminal provisions.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

If there is evidence of serious wrongdoing, the company may be left with no choice but to refer all gathered information to the authorities. It is important to keep in mind on all occasions that any report to the authorities by the company, especially in relation to its employees or clients, should be done carefully to avoid any possibility of it being held liable for filing false accusations. It is not expected, of course, that a case be presented to

© Law Business Research 2021

the authorities proven beyond any doubt, but care should be taken to forward information that indicates with some certainty that serious misconduct has taken place.

Self-reporting may extend to third countries, when there is favourable legislation regarding self-reporting from which the company could benefit (e.g., if the company could reach a leniency or immunity agreement under certain conditions).

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The first step is to gather and secure all evidence regarding the alleged wrongdoing. Next, a detailed report should be drafted to explain, with some certainty, that serious misconduct has taken place. Finally, the report is filed with the Prosecutor's Office or other competent authority.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

In principle, a company must co-operate with the authorities, at least in terms of providing requested information and documentation. Failure to comply with such a request usually has no direct consequences (unless otherwise provided for by law) but may lead to an unfavourable report by the authorities or an on-site search and seizure to obtain the requested material.

In practice, a company's attorney (in-house counsel or an independent attorney) liaises with the authorities and informs them whether or not the company will comply with the notice or subpoena, and requests additional information regarding the scope of the investigation and its purpose.

55 Are ongoing authority investigations subject to challenge before the courts?

Although it is not common, the validity of investigative actions, such as searches and seizures, may be challenged before the Judicial Council, according to the provisions of the Code of Criminal Procedure (CCP).

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

When multiple jurisdictions are involved, an international instrument or treaty may be applicable in the first instance. If the relevant jurisdictions are all EU Member States, EU law is applied; this is very similar to Greek law on the basic elements of procedure. If a bilateral or international treaty is in force (in relation to other countries), the provisions of the treaty are primarily applied. Treaties usually have specific provisions on how to

© Law Business Research 2021

handle privileged information or private data but, in some cases, Greece reserves the right to refuse to forward requested information if it is against Greek law, or may reserve the right to forward it, subject to approval from the competent authority (e.g., dealing with protection of private data).

In large-scale investigations involving more jurisdictions, all investigations are usually carried out locally in accordance with Greek law and regulations. Exceptions may apply in cases involving national security or relating to Greece's diplomatic relations, in which case different rules (as set out in international or bilateral treaties) may apply.

A company can always notify the authorities in different jurisdictions of a current investigation in Greece, to avoid multiple prosecutions or sanctions and a potential breach of the *ne bis in idem* principle.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In principle, companies are not obliged by law to comply with requests from the authorities to produce evidence. However, it is advisable for companies to co-operate with the authorities, at least in terms of providing requested information and documentation, to avoid unfavourable reports by the authorities or an on-site search and seizure to obtain the requested material. Regarding the production of material located in other countries, a company must decide whether to comply with such requests, primarily by examining whether the production of the documents would violate foreign laws (such as personal data legislation, banking secrecy laws, privileged data, etc.). If a company does not comply with a request, the authorities could still issue a European Investigation Order (for investigation within the European Union) or file a mutual legal assistance request (for investigation within third countries) to seek the requested material, which then would be gathered in accordance with the legislation of the requesting state.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Co-operation with other countries' law enforcement or prosecutorial authorities has become common practice in large-scale investigations. Special law enforcement agencies, such as the Economic and Financial Crime Unit, have entered into agreements with foreign counterparts, which has enabled a faster and more efficient exchange of information. Agreements between agencies usually follow framework agreements or treaties between countries. In the case of Greece, most aspects of international co-operation are treaty-based.

In recent times, there has been a marked increase in the co-operation of special prosecuting and investigating task forces with the corresponding authorities in other countries (especially in Germany and Switzerland) by adopting more flexible and quicker procedures.

© Law Business Research 2021

There are two sets of rules applicable to this prosecutorial co-operation, one of which applies to co-operation with EU Member States (in these cases, all procedures and functions are simplified and faster). In all other cases, provisions for mutual assistance apply (for investigating acts or requests for information).

Greece is a party to numerous international and European conventions and bilateral agreements covering all aspects of cross-border judicial co-operation, such as:

- the European Convention on Mutual Assistance in Criminal Matters (1959);
- the European Convention on the suppression of terrorism (1977);
- the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990);
- the Convention of the Council of Europe against Corruption (1999);
- the UN Convention against Transnational Organized Crime (2000);
- the UN Convention against Corruption (2003);
- the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005); and
- bilateral agreements with the United States, China, Poland, Mexico and other countries.

Greek courts co-operate with those of other EU Member States through the Eurojust agency.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Under the CCP, investigation proceedings are non-public; secrecy towards third parties and the public applies to all information gathered by the enforcement authorities. Only the person under investigation and the authorities have access to this information. Information gathered is not disclosed to third parties unless they have a specific legitimate interest to obtain the information, following special authorisation by the prosecuting authorities.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should inform the Greek authorities that complying with such a request would be illegal under the laws of that third country. Thus, the Greek authorities would decide whether to obtain the evidence through official channels (such as filing a request for mutual assistance).

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

According to Article 212 of the CCP, information in the possession of clerics, lawyers, doctors, pharmacists and military diplomatic officials is considered privileged. If an

© Law Business Research 2021

individual under investigation declares that certain documents are privileged information pursuant to Article 212 of the CCP and the investigating authority contests this assertion, the confiscated documents are sealed, without the investigating authority acquiring knowledge of their content, and a request is submitted to the competent professional association to decide on the confidentiality of the documents.

This restriction does not apply if the person protected by privilege is under investigation as an accomplice to a criminal act.

In criminal proceedings, as opposed to administrative or tax proceedings, there is no general legal framework governing the co-operation of a private legal entity with the investigating authorities (except when explicitly stated by law). In this respect, companies are not obliged to carry out the investigating authorities' requests to provide evidence, unless stated otherwise by law (e.g., telecommunications companies are obliged to provide data, when requested by a prosecutor or the investigating judge). However, 'passive' co-operation is expected when searches are conducted at the premises of companies; in other words, a company is not allowed actively to hinder searches conducted at its offices, such as by destroying evidence.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

As a general rule, material requested by the prosecuting authorities during the process of a criminal investigation must be produced. If part of this material contains privileged information, there are procedures under the CCP for handling this information accordingly. Most privileges do not apply in investigations into corruption. The Anti-Corruption Prosecutor, the Financial Crime Prosecutor and certain agencies, such as the Economic and Financial Crime Unit, may have full access to most of the privileged information. Production of material by third parties is also taken into consideration if they have legal access to it and it is not gathered or accessed through violation of criminal provisions (e.g., illegal recording of conversations or illegal access to personal data).

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Depending on the nature of the misconduct, a broad variety of administrative sanctions may be imposed against a company, such as fines, licence revocation, a permanent or temporary ban from public tenders or state funding, or a temporary suspension of business operations.

Individuals may face criminal penalties (which may include imprisonment and monetary penalties) if they are found guilty of a criminal offence.

It should be noted that crimes relating to an entity may be committed by members of the entity (usually managers, officers and directors). These individuals are personally liable in any case, but they cannot be held liable for criminal acts 'committed' by the entity

© Law Business Research 2021

if they do not meet the criteria (objective and subjective) of the relevant legal provision. For some types of offences (e.g., relating to tax matters), there are special provisions as to which persons are deemed liable under the relevant law. These legal provisions may expand or restrict liability to individuals holding certain positions within an entity.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Suspension and debarment of a company from government contracts in Greece is an administrative penalty that can be found in various laws:

- Under Article 45 of Law 4557/2018 regarding money laundering, failure to comply with the Law's anti-money laundering provisions may lead to the corporation being prohibited from carrying out certain activities, establishing new branches in Greece or abroad, or increasing its share capital. In the case of serious or repeated violations, failure to comply may result in final or provisional withdrawal or suspension of authorisation of the corporation for a specific time or prohibition from carrying out its business.
- Under Article 28, paragraph 5 of Law 1650/1986 (as amended by Article 7, paragraph 4 of Law 4042/2012) regarding the protection of the environment, a company may be banned temporarily or permanently from public tenders if it is found liable for polluting or degrading the environment to gain illicit profits.
- Under Article 24 of Law 3340/2005 for the protection of the capital market from actions of persons that possess inside information and market manipulation, the activities of a company found to be violating the provisions of this Law may be suspended.

A company should primarily examine whether the intended settlement in another country concerns facts that have taken place in Greece and evaluate the risk of that settlement being used in future proceedings in Greece.

65 What do the authorities in your country take into account when fixing penalties?

When imposing sanctions (in the form of administrative penalties) on a corporation, the competent authorities consider the following factors: entity size and annual turnover, seriousness of the offence, the damage caused, the amount by which the company benefited from the conduct and prior misconduct. The fine is imposed by the relevant competent authority (usually the Revenue Service). Apart from a fine, the competent authority may impose additional measures, such as prohibition of business activity for a specified period, revocation of licences and registrations, or a ban from public tenders or investment programmes, among other things. Judicial control of sanctions is always available to affected parties.

© Law Business Research 2021

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No. However, alternative forms for the resolution of criminal cases involving individuals are provided for in the Code of Criminal Procedure.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Prior to any settlement with a law enforcement authority, a company should consider whether the settlement agreement could be used as evidence against individuals (i.e., directors or employees of the company) or even against the company itself in any type of proceeding (criminal, administrative or civil). Also, the company should thoroughly negotiate with the authorities regarding the wording of the settlement agreement to avoid any indirect admission of wrongdoing that is not covered by that agreement.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Regulatory agencies (such as the Competition Commission, the Capital Market Commission and the Greek Gaming Commission) monitor the adherence of corporate entities to standards set by the relevant legal provisions in respect of matters within their competence. In the event of breaches, these agencies have the powers to impose administrative penalties and to forward their findings to the Prosecutor's Office for a criminal investigation to be initiated.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes, private actions seeking damages in the course of civil proceedings are allowed. Private plaintiffs may gain access to authorities' files, provided they can adequately prove their legitimate interest in obtaining the files to support their civil claims against the company.

© Law Business Research 2021

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under Article 241 of the Code of Criminal Procedure (CCP), the pretrial stage of proceedings, which includes the preliminary inquiry and the main investigation, is conducted in secrecy, not publicly. However, in highly publicised cases, it is not unusual that information (including, inter alia, documentary evidence and witness statements) is leaked to the media during the investigation phase.

After a case has been referred for trial, all procedures, including the trial hearing, are, as a rule, in the public domain (CCP, Article 329).

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There is no standard corporate communication protocol in Greece, thus companies would usually follow the international standards regarding communications in crisis management. However, it is common for companies to have their own public communications and media department. In some cases, companies also use public relations firms to help manage a corporate crisis.

73 How is publicity managed when there are ongoing related proceedings?

Companies decide on how to manage publicity case by case. Crucial factors that help to develop a company's strategy are the nature of the proceedings and the company's involvement regarding the facts under investigation and the investigated persons.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

No, but it may be advisable in some circumstances.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Each ESG area is regulated by its respective laws. In particular, environmental matters are regulated by Law 1650/1986 regarding the protection of the environment; social matters are primarily governed by labour law provisions; and corporate governance is regulated by Law 4706/2020.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

No fundamental changes are expected.

© Law Business Research 2021

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

No.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

No fundamental changes are expected.

© Law Business Research 2021

14

Hong Kong

Donna Wacker, Jonathan Wong, Anita Lam, William Wong and Michael Wang[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The Hong Kong Securities and Futures Commission (SFC) remains active in pursuing alleged corporate misfeasance by listed companies, as well as members of their current or former senior management. As noted in its 2021 Annual Report, the SFC commenced three civil and market misconduct tribunal proceedings in the reporting year against listed companies suspected of embellishing their financial statements or sales revenue in the listing prospectus and entering into overpriced acquisitions, and against directors allegedly siphoning off assets. In the same year, for similar misconduct, disqualification orders of between three and nine years were obtained against former officers and senior executives in three cases (*Shandong Molong*, *EganaGoldpfeil* and *Long Success*). Shandong Molong was further ordered to reconstitute its audit committee and, as against the relevant directors of EganaGoldpfeil, compensation of HK$622 million was ordered. The Stock Exchange of Hong Kong Limited also revised its Listing Rules to enhance its disciplinary powers and sanctions, including introducing secondary liability on relevant parties such as senior management, and a new sanction in the form of a public statement that, in its opinion, a director is unsuitable to occupy the position, indicating its continued focus on misconduct by individuals. Further, there are developments as far as the Financial Reporting Council (FRC) is concerned, which, among other things, seeks to improve

1 Donna Wacker and Jonathan Wong are partners, and Anita Lam, William Wong and Michael Wang are consultants at Clifford Chance. They acknowledge the assistance of colleague Felicia Cheng, a professional support lawyer at Clifford Chance. This chapter does not consider the implications of the Hong Kong National Security Law.

© Law Business Research 2021

the overall quality of audits performed on Hong Kong-listed companies. In October 2021, the FRC commenced an inquiry into the financial statements of China Evergrande Group and an investigation into the audit carried out by PricewaterhouseCoopers (PwC) identifying questions about the adequacy of going concern reporting.

One of the SFC's top enforcement priorities in 2020 and 2021 was combating online 'ramp and dump' schemes. In March 2021, the SFC and the Hong Kong Police Force (HKPF) conducted a joint operation against a syndicate suspected of operating ramp and dump schemes involving suspected fraud and money laundering offences in addition to market misconduct offences under the Securities and Futures Ordinance (Cap. 571) (SFO). Twelve people, including those believed to be the ringleaders, were arrested during a joint search of 27 premises across Hong Kong. Prior to the operation, 16 restriction notices had been issued and HK$860 million in assets frozen. This was followed by a further joint operation in April 2021 involving a search of office premises of a Hong Kong-listed company. Three senior executives were arrested for allegedly conspiring to use bogus transactions to embezzle funds. Other than money laundering, corruption may also be involved in ramp and dump schemes. This is illustrated by a joint operation in July 2021 conducted by the SFC and the Independent Commission Against Corruption (ICAC) concerning a suspected ramp and dump scheme. A senior executive of a listed company was arrested for suspected associated corruption offences while the operation involved a search of the offices of the listed company and one of its underwriters in its initial public offering.

There continues to be a focus on anti-money laundering (AML) and counter-terrorism financing. A record fine in the region of HK$2.7 billion was imposed by the SFC in October 2020 for serious lapses and deficiencies in AML controls in the context of bond offerings by 1Malaysia Development Berhad. In 2020 and up to July 2021, there were five other cases involving AML control failures leading to fines of between HK$3.7 million and HK$25.2 million.

The SFC works closely with the ICAC. Following a joint operation with the SFC, the ICAC charged a number of former executive directors of Convoy Global Holdings Limited, and managers, with conspiracy to defraud in July 2019. In October 2021, they were convicted and sentenced to between four and seven months' imprisonment. Two former executive directors were also disqualified from being company directors for three years and two years, respectively.

There is also continued close co-operation between the SFC and the Mainland Chinese regulators, including the China Securities Regulatory Commission (CSRC) and the China Banking Regulatory Commission. As a recent example, the CSRC assisted the SFC in the latter's investigation of Shandong Molong, as discussed above.

2 Outline the legal framework for corporate liability in your country.

The law of Hong Kong has followed the common law of England and Wales in ascribing corporate liability for criminality, and has developed two main techniques for attributing to a corporate the acts and states of mind of the individuals it employs:

- the 'identification principle', whereby, subject to some limited exceptions, a corporate entity may be indicted and convicted for the criminal acts of the directors and managers who represent its directing mind and will, and who control what it does; and

© Law Business Research 2021

- vicarious liability, under which a corporation is liable for the criminal acts of its employees or agents under statutory offences that impose an absolute duty on the employer.

A number of offences in Hong Kong legislation target corporates and regulate business activity. They include offences provided in the Companies Ordinance, the SFO, the Trade Descriptions Ordinance and the Theft Ordinance.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are subject to investigation or regulation by a number of authorities, including the ICAC, the HKPF, the Customs and Excise Department, the Companies Registry, the Inland Revenue Department, the SFC, the Hong Kong Monetary Authority (HKMA), the Insurance Authority (IA), the Competition Commission and the Office of the Privacy Commissioner (OPC).

By way of illustration of the allocation of jurisdiction between Hong Kong authorities, regulation by the SFC and the HKMA of registered institutions and their executive officers and management is governed by the 2002 memorandum of understanding, as amended in 2004. For example, the SFC has the statutory power to discipline a former relevant individual. In November 2020, the SFC banned a former relationship manager of two banks from re-entering the industry for 21 months following investigation and referral by the HKMA for failing to disclose personal securities accounts and conducting securities transactions without clearance or reporting. In May and September 2020, following referral by the HKMA, the SFC reprimanded and fined two banks HK$7 million and HK$4.2 million respectively for control failures in relation to the sale of collective investment schemes and the failure to segregate client and proprietary securities in custodian accounts.

Hong Kong's Department of Justice (DOJ) has overall responsibility for conducting criminal prosecutions; the other authorities named above conduct investigations and sometimes carry out prosecutions, depending on the offences involved. For example, the SFC is only empowered to prosecute offences under the SFO in the magistrates' courts, where the power to impose penalties is more restricted. The SFC is required to refer cases to the DOJ for prosecution of offences under the SFO in the District Court and the Court of First Instance: in August 2020, criminal prosecution was commenced for offences under the SFO against five individuals involved in alleged false trading of shares of Ching Lee Holdings Limited in the Court of First Instance for a trial by jury, which is the first of its kind. There has also been an increase in co-operation between law enforcement authorities in mounting joint investigations. The SFC signed memorandums of understanding with the IA in September 2020 to cover case referrals, joint investigations and information sharing following the introduction of direct regulation of insurance intermediaries and to facilitate supervision of entities and financial groups of regulatory interest to both regulators, and with the Financial Reporting Council (FRC) in February 2021 to improve the overall quality of audits performed on Hong Kong-listed companies by sharing expertise and resources, including in joint investigations. The FRC (Amendment) Bill 2021 was passed by the Legislative Council on 22 October 2021. It

© Law Business Research 2021

will take effect after it is signed by the Chief Executive and promulgated by way of publication in the Gazette as an ordinance; the date of operation will be a day to be appointed by the Secretary for Financial Services and the Treasury. The Bill transfers regulatory powers from the self-regulating Hong Kong Institute of Certified Public Accountants to the independent FRC, which will become the Accounting and Financial Reporting Council (AFRC). The AFRC will regulate public interest entity or listed company auditors, including exercising powers of inspection, investigation and discipline, and certified public accountants and practice units.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In general, criminal authorities must have reasonable grounds to suspect that a crime has been committed before starting an investigation. The threshold of suspicion is relatively low.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A challenge to a search and seizure warrant or production order, and a request to exclude evidence gathered as a result, can be made based on scope, the grounds on which the order was obtained, legal professional privilege or public interest grounds through an application to the Hong Kong courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Deferred prosecution agreements (DPAs) are commonly used by prosecutors and regulators in the United States and the United Kingdom. Although they have not been formally introduced in Hong Kong, different Hong Kong regulators have, in practice, their own co-operation arrangements. For example, the ICAC or the HKPF from time to time grant perpetrators immunity from prosecution in return for co-operation, after consultation with the DOJ. Both the SFC and the HKMA have published guidance notes on co-operation in investigations and enforcement proceedings under which a person may obtain a credit on the disciplinary penalty if they settle with the regulators. These guidance notes do not apply to criminal cases over which the DOJ has sole discretion. It is also common for the SFC or the HKMA to require, as a part of a settlement, the appointment of an independent reviewer, who may perform a role similar to a that of a monitor under DPAs in the United States or the United Kingdom.

7 What are the top priorities for your country's law enforcement authorities?

The HKPF's priorities are syndicated and organised crime, money laundering and 'quick cash' crime (e.g., theft, extortion and deception). The HKPF is also prioritising cybersecurity and technology crime, particularly through the internet and social media.

© Law Business Research 2021

The SFC's enforcement priorities include investment fraud and online investment scams, including ramp and dump schemes, corporate misfeasance and fraud by listed companies or senior management (such as listed companies embellishing their financial results or directors misappropriating assets), intermediary misconduct and money laundering.

The HKMA's priorities include risk management relating to money laundering and the financing of terrorism, digitalisation including remote customer onboarding and non-face-to-face distribution, operational and cyber resilience, management of online fraud and financial crime risk, green and sustainable banking, smooth transition away from the London Inter-Bank Offered Rate (LIBOR) and credit risk.

The IA focuses on protecting and promoting the rights and interests of policyholders and facilitating the sustainable development of the insurance industry both in Hong Kong and regionally. From 23 September 2019, the IA took over regulation of insurance intermediaries from three self-regulatory organisations and delegated certain inspection and investigation powers to the HKMA with respect to insurance-related businesses carried on by authorised institutions. The group-wide supervision framework came into effect in March 2021 providing for regulation of multinational insurance groups through power over Hong Kong-incorporated holding companies.

The ICAC continues with a relatively even focus on combating corruption in both the public and private sectors. In terms of corruption complaints recorded in 2020, 41 per cent concerned government departments and public bodies and 59 per cent concerned the private sector. The areas attracting the most complaints in the private sector were building management, construction, finance and insurance. The ICAC also has a proceeds of crime section to deal with restraint, disclosure and confiscation of assets under the Organised and Serious Crimes Ordinance (Cap. 455) and provided input to the HKPF regarding the money laundering threat in respect of the predicate offence of corruption.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Save for the financial industry, which is heavily regulated, and Hong Kong-listed companies (although these are not directly regulated by a law enforcement authority, per se), Hong Kong does not have statutorily mandated compliance programmes that are required of all corporations generally, and there is no statutory leniency offered to corporations with a compliance programme. That notwithstanding, it is good practice to have an effective compliance programme in place, and some law enforcement authorities, such as the ICAC, have published guidance encouraging corporations to set up such programmes.

In respect of the financial industry, for persons licensed by or registered with the SFC, one of the nine general principles in the Code of Conduct is compliance. Paragraph 4.3 of the Code of Conduct provides that a licensed corporation should have internal control procedures that reasonably protect operations, clients and other persons from financial loss occasioned by theft, fraud and other dishonesty, as well as from professional misconduct, and the SFC has issued the Management, Supervision and Internal Control

© Law Business Research 2021

Guidelines (April 2003) to provide further guidance with respect to the SFC's expectations in relation to internal controls. Similarly, with respect to authorised institutions (i.e., banks and deposit-taking companies), the HKMA has issued a Supervisory Policy Manual on Risk Management Frameworks, which provides that banks are expected to have a programme in place to ensure compliance with applicable statutory provisions, regulatory requirements and codes of conduct.

Listed companies are subject to the Listing Rules, appended to which is the Corporate Governance Code (the CG Code), which covers such areas as board practice and composition; director remuneration and responsibilities; delegation; supply of information to directors; financial reporting; audit committee; company secretary; and communication with shareholders. It sets out the principles of good corporate governance at two levels: code provisions and recommended best practices. The CG Code adopts the comply or explain approach; listed companies must state whether they have complied with the code provisions in their interim and annual reports and, if they have not, give considered reasons. This approach is encouraged, but not required, for recommended best practices. The CG Code provides that the board is responsible for determining the nature and extent of the risks it is willing to take in achieving the listed company's strategic objectives, and ensuring the listed company establishes and maintains appropriate and effective risk management and internal control systems. The board should oversee management in the design, implementation and monitoring of these systems. The board should ensure that a review of the effectiveness of the systems is conducted at least annually, and report to shareholders that it has done so, and whether the listed company considers the systems effective and adequate in its corporate governance report. The review should cover all material controls such as financial, operational and compliance. Failure to report will be regarded a breach of the Listing Rules.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

There is no overarching legal framework for cybersecurity in Hong Kong. Entities regulated by the Hong Kong Securities and Futures Commission (SFC), Hong Kong Monetary Authority (HKMA) and Insurance Authority (IA) must abide by the various guidelines and circulars concerning cyber risk management, resilience testing and management accountability.

In October 2017, the SFC published guidelines requiring all licensed corporations engaged in internet trading to implement 20 baseline requirements covering preventive, detection and internal governance-related controls. At the same time, the SFC issued a circular advising that the guidelines are only minimum standards and senior management should ensure that all systems and controls are commensurate with business needs and operations, and implement additional cybersecurity controls as necessary. Under the April 2003 Management, Supervision and Internal Control Guidelines of the SFC, licensed persons are required to implement an effective business continuity plan

© Law Business Research 2021

appropriate to their size to ensure that they are protected from interruption risk, which may arise from a cyberattack.

The HKMA issued a circular in September 2015 stating that senior management should evaluate periodically the adequacy of an authorised institution's cybersecurity controls having regard to emerging cyber threats and credible cybersecurity control benchmarks. The circular also pinpointed the need for contingency planning and independent assessment. In May 2021, the HKMA issued a further circular requesting critical assessment of the need for secure tertiary data backup to counter the risk of cyberattacks. In addition, the HKMA launched a Cybersecurity Fortification Initiative (CFI), one of the pillars of which is the Cyber Resilience Assessment Framework (C-RAF). An upgraded CFI (CFI 2.0) came into effect on 1 January 2021. There is a timeline for authorised institutions to complete their C-RAF 2.0 assessments. C-RAF 2.0 encompasses enhanced control principles reflecting the latest developments in overseas cyber practices in relation to cyber incident response and recovery.

The IA published a guideline on cybersecurity (GL 20) in June 2019, which sets out the minimum standard for cybersecurity that authorised insurers are expected to have in place.

The Personal Data Privacy Ordinance (PDPO) addresses the security of personal data, including data storage and security measures.

Large-scale cybersecurity failings resulting in breach of personal data protection rules are treated seriously by regulators. The Office of the Privacy Commissioner regularly carries out investigations of such failings and issues enforcement notices. Failure to comply with these notices may lead to criminal sanctions.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

There are a number of offences under Hong Kong law targeting cybersecurity-related crimes, including unauthorised access to a computer by telecommunications under the Telecommunications Ordinance and access to a computer with criminal or dishonest intent under the Crimes Ordinance. Other offences that may be applied to prosecute cybercrime include criminal damage under the Crimes Ordinance and theft under the Theft Ordinance.

The Cybersecurity and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force is responsible for carrying out investigations into technology crime, including computer forensic examinations. The CSTCB also liaises closely with local and overseas law enforcement agencies on combating cross-border technology crime. For example, the CSTCB conducted a joint investigation with the Singapore Police Force into a transnational online credit card fraud syndicate, which stole card details via phishing. Five core members of the syndicate were arrested in July 2020. In terms of exchange of experience, CSTCB and Interpol co-hosted a technology crime investigation workshop in July 2021 and the Chief Superintendent of CSTCB chaired the annual meeting of the Interpol Global Cybercrime Expert Group in the same month.

© Law Business Research 2021

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The primary basis of criminal jurisdiction in Hong Kong is territorial, and the courts apply a strong presumption against construing statutes as having extraterritorial effect.

The Criminal Jurisdiction Ordinance (CJO) deals with Hong Kong's extraterritorial criminal jurisdiction. The offences to which the CJO applies are divided into Group A offences, which include theft, fraud, deception, blackmail and offences relating to false instruments, and Group B offences, which cover conspiracy, attempting or incitement to commit a Group A offence, and the offence of conspiracy to defraud.

The CJO allows Hong Kong courts to exercise jurisdiction over offences under both groups in the following circumstances:

- any of the constituent elements of the offence occurs in Hong Kong; or
- there is an attempt to commit the offence in Hong Kong, whether or not the attempt is made in Hong Kong or elsewhere and irrespective of whether it has an effect in Hong Kong; or
- there is an attempt or incitement in Hong Kong to commit the offence outside Hong Kong; and
- the substantive offence was not intended to take place in Hong Kong.

As regards a conspiracy to commit a Group A offence, or conspiracy to defraud, jurisdiction depends on proof that the pursuit of the agreed course of conduct would involve conduct punishable under the law in force in the place where the conduct was intended to take place. The prosecution must also prove that:

- a party to the agreement constituting the conspiracy, or a party's agent, did something in Hong Kong in relation to the agreement before its formation; or
- a party to the conspiracy became a party in Hong Kong (by joining it either in person or through an agent); or
- a party to the conspiracy, or a party's agent, did or omitted to do anything in Hong Kong in pursuance of it; and
- the conspiracy would be triable in Hong Kong, but the parties to it had not intended that the offence or fraud would take place in Hong Kong.

In relation to conspiracies to commit all other offences, section 159A of the Crimes Ordinance codifies the general common law rule limiting extraterritorial jurisdiction in conspiracy cases and provides that conspiracies entered into in Hong Kong are triable in Hong Kong only if the agreement is to commit substantive offences that are triable in Hong Kong. Conspiracies entered into abroad to commit substantive offences in Hong Kong would be triable in Hong Kong even before any acts were carried out within the territory in furtherance of the conspiracies. However, conspiracies entered into in Hong Kong to commit offences abroad would not be triable in Hong Kong.

© Law Business Research 2021

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations may touch on Hong Kong's data privacy regime, or regimes of other countries in Asia, such that employee or customer consent may be required prior to disclosing certain protected information. Cross-border investigations involving China should be conducted in compliance with the Chinese Law on Guarding State Secrets, Chinese Cybersecurity Law and Chapter VI of the new Civil Code (which concerns personal data privacy), which into effect on 1 January 2021. A new Data Security Law in China has also been passed and takes effect in September 2021. It regulates data activities to protect and promote state security and development. It purports to have extraterritorial effect applying to data activities outside China that may harm national security or public interests, or the legitimate rights of Chinese citizens or entities. Further, the new Personal Information Protection Law takes effect in November 2021, which also purports to have extraterritorial effect governing offshore processing of personal information of individuals in China in relation to the provision of goods or services to, or analysis of activities of, such individuals. In certain cases, investigators may need to undertake their work on site in China with strict protocols in place to prevent the prohibited export of information to Hong Kong or elsewhere.

In July 2019, the Chinese Ministry of Finance (MOF), the China Securities Regulatory Commission (CSRC) and the Hong Kong Securities and Futures Commission (SFC) entered into a memorandum of understanding concerning the obtaining of audit working papers in China. The aim of this is to facilitate the SFC's access to these documents when conducting investigations into Chinese companies listed in Hong Kong and their related entities or persons. Under the memorandum of understanding, the MOF and the CSRC will provide the fullest assistance in response to requests by the SFC for investigative assistance regarding the provision of audit working papers. The Financial Reporting Council (FRC) also has a May 2019 memorandum of understanding with the Supervision and Evaluation Bureau of the MOF under which it may obtain assistance for the provision of audit working papers. In July 2021, the FRC completed its first investigation report using audit working papers obtained thereunder in relation to a failure by the auditor of a listed entity to identify a material misstatement in the consolidated financial statements. A second investigation report using audit working papers similarly obtained was completed in August 2021, involving a similar failure.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The right of an accused to advance double jeopardy is found in the Hong Kong Bill of Rights Ordinance and the Criminal Procedure Ordinance. This protection extends to

© Law Business Research 2021

corporations convicted or acquitted of an offence abroad. There is no express or specific legislation or regulation analogous to the 'anti-piling on' policy as exists in the United States.

14 Are 'global' settlements common in your country? What are the practical considerations?

Regarding global settlements involving more than one country, there are no published figures on their prevalence. The SFC has co-operative arrangements for investigatory assistance and exchange of information with many overseas regulators. In particular, the CSRC and the SFC have maintained a close strategic partnership to tackle cross-border trading misconduct. The Hong Kong Monetary Authority has co-operative arrangements with the People's Bank of China and the China Banking and Insurance Regulatory Commission to ensure cross-border banking operations are effectively controlled and prudently conducted. The Insurance Authority has co-operative arrangements with the China Insurance Regulatory Commission to enhance insurance supervision and co-operation against insurance fraud.

When handling 'global' settlements, practical considerations include ensuring information parity between regulators and coordinating the timing of publishing or announcing the settlement in different jurisdictions.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

To facilitate investigation of the same matter, the Hong Kong authorities generally try to co-operate with their counterparts in foreign jurisdictions and in China. For example, in October 2014, the SFC and the CSRC entered into a memorandum of understanding on strengthening cross-boundary regulatory and enforcement co-operation with a view to tackling market manipulation in China and Hong Kong. Furthermore, the MOF, the CSRC, the SFC and the FRC entered into memoranda of understanding on audit working papers.

In addition, Hong Kong has mutual legal assistance agreements with a number of countries, and a number of international treaties provide for cross-border co-operation.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Hong Kong generally adheres to United Nations Security Council sanctions, including pursuant to the Weapons of Mass Destruction (Control of Provisions of Services) Ordinance, the United Nations Sanctions Ordinance and the United Nations (Anti-Terrorism Measures) Ordinance with oversight by the Chinese Ministry of Foreign Affairs. Hong Kong does not impose unilateral or autonomous sanctions. There was some discussion in August 2021 that China's Anti-Foreign Sanctions Law would be introduced into the laws of Hong Kong but that had not happened at the time of writing. It was reported that China's government had decided not to proceed with the plan for the time being.

© Law Business Research 2021

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Multiple agencies share responsibility for the administration and enforcement of Hong Kong sanctions, including the Chief Executive, the Hong Kong Department of Justice, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Commerce and Economic Development Bureau, the Customs and Excise Department, and the Trade and Industry Department. Although regulatory focus has increased, particularly for the financial sector, there have been no notable cases of criminal enforcement of sanctions breaches in Hong Kong in recent years.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Hong Kong has a variety of mutual legal assistance arrangements with foreign jurisdictions, which may be used in support of sanctions-related investigations.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Hong Kong has no such legislation, albeit China enacted its Anti-Foreign Sanctions Law in June 2021. There was some discussion in August 2021 that China's Anti-Foreign Sanctions Law would be introduced into Hong Kong's Basic Law by the Standing Committee of the National People's Congress in that month, but that had not happened at the time of writing. It was reported that China's government had decided not to proceed with the plan for the time being.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Whistleblower complaints, both internal and external, are a frequent source of allegations of misconduct leading to investigations, particularly with respect to bribery and corruption. The role of the Independent Commission Against Corruption (ICAC) in receiving and investigating complaints made against individuals is critical. Enquiries by the ICAC to companies regarding their employees' conduct will often lead to an internal investigation to identify potential breaches of internal policy even when there is no corporate liability under the law.

© Law Business Research 2021

Where there is known or suspected money laundering or terrorist financing, suspicious transaction reports (STRs) are required to be filed with the Joint Financial Intelligence Unit (JFIU). The JFIU, jointly run by the Hong Kong Police Force and Hong Kong Customs and Excise Department, manages the STR regime, receiving and analysing reports and disseminating them to appropriate law enforcement agencies (and financial intelligence units) in and outside Hong Kong.

Regulatory reviews by the Hong Kong Securities and Futures Commission (SFC), the Hong Kong Monetary Authority (HKMA) or other regulators are another source of allegations of misconduct. Further, corporations and institutions licensed by the SFC or the HKMA have an obligation to report material breaches (or suspected breaches) of any law, rules or regulations (including suspected misconduct) to their regulators. Specifically, corporations licensed by the SFC are expressly required to report material breaches (or suspected breaches) of market misconduct provisions under the Securities and Futures Ordinance (Cap. 571) by their clients.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Hong Kong has a data protection regime that has been given statutory force through the Personal Data Privacy Ordinance (PDPO). The PDPO applies to any data relating directly or indirectly to a living person from which it is possible to identify that person and the data is in a form in which access or processing is practicable. The PDPO contains six data protection principles (DPPs) that govern the purpose and manner of collection, the accuracy and duration of retention, the use and security of personal data, and rights of access and correction.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Contravening a DPP may give rise to a complaint to be investigated by the Office of the Privacy Commissioner (OPC). A data user may be punished under the PDPO for failing to comply with an enforcement notice issued by the Privacy Commissioner for Personal Data, after a finding of a contravention. An enforcement notice may direct the data user to take steps to remedy the contravention and prevent a recurrence. A data user may separately bring a civil claim for damages on the basis of a contravention of a DPP, whether or not the Privacy Commissioner has issued an enforcement notice.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The provisions of the PDPO cover the monitoring and gathering of data in the context of internal investigations, whether this be by monitoring the internet, public social media posts, telephone calls, chats, emails or other internal communication channels. An individual who suffers damage (including 'injured feelings') by reason of a breach may sue. The Personal Data (Privacy) (Amendment) Ordinance 2021 (PDPAO), which criminalises doxxing, came into effect on 8 October 2021. The new offences cover criminalisation of

© Law Business Research 2021

the disclosure of personal data without the data subject's consent where the disclosing party has an intent to cause harm, or is reckless in regard to causing harm, such as harassment or pestering, bodily or psychological harm, or damage to property. The PDPAO also empowers the OPC to serve notices to cease or restrict disclosure of doxxing content and carry out criminal investigation, and failure to comply or co-operate with the same may lead to a criminal offence. Further guidance from the OPC on the application of the law in the context of legitimate whistleblowing and employment-related internal investigations would be helpful.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Interception of communications and covert surveillance are regulated by the Interception of Communications and Surveillance Ordinance and can only be exercised by the Customs and Excise Department, the Hong Kong Police Force and the Independent Commission Against Corruption with prescribed authorisation.

Monitoring and surveillance of employee communications is regulated by the PDPO. Prior to implementing any surveillance system, an employer must take such steps as are reasonable, in the circumstances, to ensure its employees are aware of (among other things) the fact that the information is being collected and the purpose of collection.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Dawn raids are used by the Securities and Futures Commission (SFC) and the Hong Kong Monetary Authority (HKMA) in the context of regulatory investigations, by the Independent Commission Against Corruption in bribery investigations and by the Hong Kong Police Force in relation to the commission of any offence. Dawn raids may also be used by the Competition Commission in investigating offences under the Competition Ordinance. They can take place either with a warrant issued by a magistrate or without a warrant in limited circumstances. The Office of the Privacy Commissioner has been given dawn raid powers for certain offences relating to disclosure of personal data without consent and with specified harmful intent under the proposed Personal Data (Privacy) (Amendment) Ordinance 2021, which came into effect on 8 October 2021.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Generally, privileged material cannot be seized during a dawn raid or in response to a search warrant. To protect privileged material from seizure, a claim of privilege should be made, and if there is a dispute as to whether certain material is privileged, the material should be sealed until the dispute is resolved. However, privilege may be overridden by a

© Law Business Research 2021

court order. Privilege will also not attach to material created for the purpose of committing a crime.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Privilege against self-incrimination is recognised in Hong Kong. A person may decline to provide information in an investigation that may lead to self-incrimination.

An exception is that authorities such as the SFC and the HKMA may issue a notice under relevant statutory provisions compelling a witness to answer questions or produce documents, and self-incrimination is not a reason for non-compliance. However, the information provided by the person compelled by the notice will be inadmissible in evidence against the person in criminal proceedings except for certain offences, such as perjury.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Hong Kong currently does not have a comprehensive or overarching framework to protect whistleblowers and the legal protections for whistleblowers are limited. There are no financial incentive schemes for whistleblowers to volunteer information. However, listed companies are encouraged to adopt a whistleblowing policy as 'recommended best practice' under the Corporate Governance Code (the CG Code) of the Stock Exchange of Hong Kong Limited (the Exchange). In the Exchange's April 2021 consultation paper, it proposed that the adoption of a whistleblowing policy be upgraded from a recommended best practice to a provision in the CG Code. The Hong Kong Monetary Authority (HKMA) also advised in its March 2017 bank culture reform circular that authorised institutions should put in place a whistleblowing mechanism to facilitate timely reporting of any illegal, unethical or questionable practices in a confidential setting without the risk of reprisals. This message was repeated in the HKMA's May 2020 circular reporting on its review of bank culture self-assessments, with the HKMA stating that more work was needed to promote an environment that provides psychological safety to encourage staff to speak out without fear of adverse consequences.

Under the Employment Ordinance, an employee giving evidence in proceedings or in response to enquiries in connection with the enforcement of the Employment Ordinance, work accidents or breach of work safety legislation is protected from dismissal and discrimination.

Other ordinances covering race, gender, family status and disability also protect individuals who act against discrimination or assist with investigations against victimisation.

Hong Kong law protects individuals who disclose suspected money laundering or other crimes by preventing the disclosure from being treated as a breach of any restrictions imposed by contract, enactment or rule of conduct. Similarly, there is protection

© Law Business Research 2021

for a whistleblower against any civil liability for reporting financial irregularities or non-compliance with financial resources rules (and for listed company auditor whistleblowers for reporting fraud) under the Securities and Futures Ordinance (Cap. 571).

Under the Prevention of Bribery Ordinance, the name or address of an informer is not to be disclosed and any document that might lead to discovery of the informer must be redacted prior to disclosure in civil or criminal proceedings. The Independent Commission Against Corruption (and police) informers are entitled to witness protection under the Witness Protection Ordinance.

In April 2020, the Competition Commission in Hong Kong revised its Leniency Policy, updating the one applying to undertakings and publishing a new one for individuals. The policies are designed to encourage companies and individuals that may have engaged in illegal activity, such as bid rigging or price-fixing, to report it in exchange for leniency.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees have limited rights under local employment laws if a company conducts an investigation and may be suspended with pay if the employment contract so provides. An employee may also be suspended without pay in the limited circumstances specified in the Employment Ordinance for generally no more than 14 days. Employees are protected against wrongful, unreasonable or constructive dismissal under local legislation.

Employees have the right to a disciplinary hearing if the company handbook, manual or policy provides for it in relation to employee misconduct. Employees of government or public bodies have the right to a fair hearing.

Executive directors owe additional duties under the Companies Ordinance, the company's articles and common law. In addition to the rights they have as an employee of the company, directors also have rights under the Companies Ordinance and their company's articles with respect to the potential threat of removal or disqualification if they breach directors' duties.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

There are no statutory requirements for companies to take disciplinary steps when an employee is suspected of misconduct. However, companies' internal policies and employment contracts may adopt disciplinary procedures for their employees, which must be adhered to. Companies in regulated industries may be required to suspend or take disciplinary action against employees who carry out regulated activities. Aside from their mandatory obligations, companies may take disciplinary action or steps to investigate misconduct as part of their proper internal controls and good corporate governance.

© Law Business Research 2021

32 Can an employee be dismissed for refusing to participate in an internal investigation?

An employee may potentially be dismissed for refusing to participate in an internal investigation after failing to heed the employer's lawful and reasonable instructions and absent any protected circumstances, such as the employee taking sick leave, maternity leave, paternity leave or work injury leave.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common practice for an internal investigation to begin with the drafting of an investigation plan detailing the objectives, scope, roles and responsibilities for the investigation. A clearly defined communications plan and the protocol for maintaining legal professional privilege are also essential from the earliest stages. Increasingly, scoping documents will also identify data custodians and outline procedures for electronic document review.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Depending on the nature of the issue, necessary internal steps could be managed by a company's compliance or legal department in less serious cases, or senior management and the board of directors in more serious cases. Under the supervision of legal counsel to ensure the protection of legal professional privilege, a company should gather and secure any relevant documents and data, and interview key employees to ensure the continued availability of critical information. Corrective action plans or disciplinary measures should be adopted to address gaps or breaches in compliance controls, which may earn a company mitigation credit in any related enforcement actions. Although the authorities may not be aware of an internal issue, it is important to pay particular regard to the self-reporting obligations by corporations and institutions licensed by the Hong Kong Securities and Futures Commission (SFC) or the Hong Kong Monetary Authority (HKMA).

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Ideally, a company should have an established protocol for responding to law enforcement requests, subpoenas or dawn raids, including procedures for the preservation of relevant documents and data. The legal department should issue a preservation notice to all relevant employees immediately upon receiving a law enforcement request, or if it believes that such a request or legal proceedings may be forthcoming. Paper documents and electronic data on servers, laptops, mobile devices or other media should be

© Law Business Research 2021

collected from relevant custodians and logged under the supervision of legal counsel and the company's information technology department. Privileged communications should be segregated and clearly stamped to help prevent accidental disclosure.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is no general duty to publicly disclose the existence of an internal investigation or contact from law enforcement (indeed, most agencies impose a secrecy obligation on the subject of an investigation). The exception is in the case of a listed company when such facts would constitute price-sensitive information, as defined under the Securities and Futures Ordinance (Cap. 571) (SFO), unless exempted or when the SFC has granted a waiver (e.g., in cases involving disclosure restrictions imposed by a foreign government authority). Conversely, there are strict prohibitions against publicly reporting details of investigations by the Independent Commission Against Corruption for both listed and unlisted companies.

37 How are internal investigations viewed by local enforcement bodies in your country?

In most cases, the authorities recognise the need for, and welcome, at least initial or preliminary internal investigations carried out by corporations. Those corporations and institutions licensed by the SFC or the HKMA have a regulatory duty to self-report when there is a material breach (or suspected breach) by their employees of any law, rules or regulations (including suspected misconduct), or when there is a material breach (or suspected breach) by their clients of any market misconduct provisions under the SFO (in the case of corporations licensed by the SFC). Particular care must be taken to avoid tipping off, whereby corporations are prohibited (except with the authorities' consent) from disclosing the existence of the authorities' investigations to a third party, which may include their employees and their clients.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal professional privilege can be claimed over various aspects of an internal investigation.

Case law holds that the whole process of obtaining and giving legal advice should be privileged. Therefore, internal communications (including those between employees of a non-legal function) and materials generated during the information-gathering process of an internal investigation (such as minutes of meetings and interview notes), for the dominant purpose of obtaining and giving legal advice, could be privileged. However, legal advice privilege will not attach to communications with, or materials prepared by, a third party (unless the communications or materials are for the dominant purpose of

© Law Business Research 2021

obtaining or seeking legal advice), nor will it cover legal advice given by persons who are not legally qualified (e.g., tax accountants).

During an internal investigation, confidential communications or documents prepared for the dominant purpose of obtaining information or evidence for use in actual or reasonably contemplated litigation – even if the communications are merely for the purpose of establishing facts – will be covered by litigation privilege. To protect privilege, a company should:

- involve lawyers (whether in-house or external counsel) as soon as it is apparent that legal advice is likely to be required;
- avoid creating unnecessary records (where there is no prospect of litigation) that summarise, quote or amend the legal advice received;
- limit circulation of privileged documents on a strictly need-to-know basis;
- manage documents effectively by separating privileged and non-privileged documents; and
- ensure that all documents that are considered to be protected by legal professional privilege are clearly marked 'privileged and confidential'.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Under Hong Kong law, legal professional privilege falls into two categories:

- Legal advice privilege attaches to communications between a client and his or her legal adviser for the purposes of giving and receiving legal advice.
- Litigation privilege attaches to confidential communications between a legal adviser and his or her client, and to communications between a legal adviser or client and a third party if three conditions are met: (1) litigation is in progress or reasonably in contemplation; (2) the communications are made with the sole or dominant purpose of conducting the actual or anticipated litigation; and (3) the litigation is adversarial, not investigative or inquisitorial.

The privilege belongs to, and can only be waived by, the client and not his or her legal adviser.

In the corporate context, it is advisable to identify the employees authorised to act for the company to seek legal advice for the purposes of claiming legal advice privilege, as English and Hong Kong law have diverged in recent years on this issue.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Legal professional privilege applies equally to in-house and external counsel. However, privilege will only cover communications made by an in-house lawyer acting in a legal (not a managerial) capacity.

© Law Business Research 2021

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Legal professional privilege applies equally to advice sought from foreign lawyers if the advice is given in Hong Kong. If the advice is given from outside Hong Kong, it is possible that privilege can be asserted under Hong Kong law even if the home jurisdiction of the foreign lawyer does not recognise legal professional privilege.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of legal professional privilege (usually on a limited basis) is generally regarded as a sign of co-operation by authorities in a regulatory investigation. This is not mandatory.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The Court of Appeal in Hong Kong has confirmed that a waiver of privilege with respect to one party does not automatically mean that privilege has been waived at large and that privilege is not waived because a privileged document has been disclosed for a limited purpose. The scope of the waiver is determined by the party waiving the privilege. Where privilege is waived for a limited purpose, it is important to ensure that the terms and scope of the limited waiver are clear.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Generally, privilege will not be lost because a privileged document has been disclosed for a limited purpose.

Whether privilege can be maintained if it has been partly waived in another country will depend on several factors, including, but not limited to:

- whether the concept of limited or partial waiver is recognised in the country where privilege has been waived;
- the scope and terms of the waiver; and
- whether any statutory provision overrides privilege.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists in Hong Kong. Privilege will not be waived if privileged material is disclosed to a third party who shares a common interest in the subject matter of the privileged material. Common interest must exist at the time when the privileged material is disclosed to the third party.

© Law Business Research 2021

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Communications between a third party and the lawyer (or the client) are protected from disclosure by litigation privilege if they are made for the dominant purpose of obtaining information or evidence for use in actual or reasonably contemplated litigation. However, legal advice privilege will generally not apply to communications with third parties.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes. There is no general prohibition under Hong Kong law against interviewing witnesses as part of the information-gathering process in an internal investigation.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Legal advice privilege is often claimed for the records of internal witness interviews, if the interviews are conducted at the direction of an in-house or external legal adviser. Case law in Hong Kong suggests that a corporation may argue that legal advice privilege exists regarding such records if the interviews are conducted (or the reports are compiled) for the dominant purpose of obtaining and giving legal advice during the internal investigation. This is in contrast to the position in England, which applies a more limited definition of 'client', for example.

Litigation privilege may only be claimed if it is established that the witness interviews are conducted for the dominant purpose of use in an actual or reasonably contemplated litigation.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Whether the interviewee is an employee or a third party, it is recommended that they be informed that:

- the interview is part of a fact-finding exercise;
- the lawyer conducting the interview represents the company, not the interviewee;
- the interview is protected by legal professional privilege belonging to the company, which can choose to disclose the contents of the interview to third parties, including regulators and authorities, without the interviewee's permission;
- the interviewee may provide personal information covered by data protection laws, which will be used only for the fact-finding or review exercise. This exercise may involve sharing the interviewee's personal information with other advisers working for the company, regulators and authorities; and
- the contents of the interview are confidential and should not be shared with any other person (including other employees).

© Law Business Research 2021

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The internal interview will typically be attended by in-house legal counsel and any specialised investigation team with or without external counsel (depending on the nature and seriousness of the issues involved). Relevant documents are typically put to the witness at the internal interview for reference, comment and explanation, as necessary. There is no legal requirement that employees have their own legal representation at an internal interview, and this is not common in practice.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Generally, a person is under no positive obligation to report crimes or provide assistance to law enforcement authorities, save for suspicious transaction reports under anti-money laundering laws, which are mandatory, and certain exceptions for licensed corporations and financial institutions.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Although there is no formal arrangement or mechanism for deferred prosecution agreements in Hong Kong, it may be advisable for a company to self-report with a view to demonstrating its proactive and full co-operation with the authorities, which may militate against a decision to prosecute or be considered as a mitigating factor in sentencing.

Whether the self-report should extend to foreign countries will depend on the nature and extent of the issues involved, in particular whether it has a cross-border, regional or global element.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

A company should undertake appropriate internal investigations to ascertain the nature and extent of the issues, and to ensure the contents of any self-report are correct and not misleading (including through any material omission). It should also seek legal advice on the applicable self-reporting obligations.

For licensed corporations and financial institutions that are under a regulatory duty to self-report, a balance needs to be struck between making timely self-reports and ensuring that reports are correct and not misleading.

© Law Business Research 2021

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Hong Kong enforcement agencies, such as the Independent Commission Against Corruption and the Hong Kong Securities and Futures Commission (SFC), have extensive powers to compel information to be provided to them by corporations involved in investigations, and there is very little that can be done to challenge requests for information when they are made.

However, it would be unusual for criminal charges to be brought against a corporation without it having an opportunity to discuss the circumstances of the allegations with the enforcement agency. In financial misconduct investigations, the twin regulatory and criminal nature of the supervisory jurisdiction of the SFC and the Hong Kong Monetary Authority (HKMA) means that there would be an opportunity for representations to be made by the corporation, through its lawyers, as to the circumstances, and the proposed remediation, prior to criminal charges being brought.

55 Are ongoing authority investigations subject to challenge before the courts?

The circumstances under which an ongoing investigation could be challenged in the courts are difficult to envisage, short of provable *mala fides* on the part of the enforcement agency.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

These circumstances are most likely to arise in the context of financial regulatory investigations by regulators in different jurisdictions, or international anti-bribery enforcement under the US Foreign Corrupt Practices Act or the United Kingdom's Bribery Act. In circumstances in which the notices or subpoenas have been issued validly, justify substantive responses and relate to identical subject matter, it is advisable to adopt consistent disclosure with each agency. Further, assuming that a financial institution's operations are international in nature, coupled with self-reporting obligations imposed in other countries (most notably the United States and the United Kingdom), this usually means that some form of notification or reporting to overseas regulators would be required even in the context of an investigation that primarily concerns Hong Kong, and in the absence of any separate notices or subpoenas being issued by overseas regulators. Given the increasing prevalence of international co-operation between regulators and criminal enforcement agencies, a failure to disclose certain matters in one jurisdiction may well be apparent and seized on as an indication of inadequate compliance or co-operation.

Assuming that the investigation primarily concerns Hong Kong, it is advisable to adopt the disclosure made to the local regulators (e.g., the SFC or the HKMA) as a 'base' document in framing the appropriate disclosure to overseas regulators with reference

© Law Business Research 2021

made to the nexus with other countries (e.g., by reason of the institution's or an individual's licensing status, client impact, and so on). Care should also be taken to ensure that notification has been given to and, in appropriate cases, consent obtained from the local regulators, before overseas notification or disclosure is made. In particular, the SFC almost always insists that its written consent be obtained before a licensed corporation can disclose the existence or content of an ongoing investigation, even to an overseas regulator.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Under notices issued by the various Hong Kong enforcement agencies, companies may be required to produce material in their possession, custody, control or power, whether this is located in other countries or solely in Hong Kong, subject to having a reasonable excuse not to do so.

This may give rise to issues in some foreign jurisdictions, where the transmission of certain types of information outside that country may be prohibited by local law. In Hong Kong, exposure to criminal liability under foreign law would not constitute a reasonable excuse for non-compliance with a notice or subpoena. This applies in circumstances where a reasonable person would conclude that the Hong Kong public interest in the investigation of criminal activities outweighs any public or private interest in compliance with the foreign law. However, if there are alternative means of obtaining the documents without materially adverse consequences to the investigation, a real and appreciable risk of prosecution under foreign law would constitute a reasonable excuse for non-compliance.

A related issue arises as to the extent that the company is required to produce relevant material in the possession, custody or power of its parent, subsidiary or an associated company (which may be incorporated in other countries). In general terms, this depends on whether the company subject to investigation (the subject company) has a presently enforceable legal right to obtain the documents from such other companies without the need to obtain the consent of anyone else. This is a question of fact, which depends on whether the subject company has sufficient control over the other companies such that the documents in the possession, custody or power of the other companies can be said to be within the power of the subject company.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Hong Kong regulators, including the HKMA and the SFC, have signed memoranda of understanding to establish co-operative arrangements that include the sharing of information with foreign counterparts, including those in China. One of the most important of these is the International Organisation of Securities Commissions Multilateral

© Law Business Research 2021

Memorandum of Understanding, which was the first global information-sharing arrangement among securities regulators.

Hong Kong authorities may co-operate with their foreign counterparts reciprocally in criminal matters under the framework established in the Mutual Legal Assistance in Criminal Matters Ordinance. However, this particular legislation is not applicable to China, Macao or Taiwan.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Information provided to enforcement authorities in Hong Kong confidentially during an investigation will remain confidential, except to the extent that its use is necessary within an investigation, prosecution or regulatory enforcement. Although it may be shared with other enforcement agencies or regulators under information-sharing agreements, it would not be disclosed to other third parties without an order from a court.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

It may be possible to refuse production on the grounds that the foreign illegality constituted a reasonable excuse not to produce the documents under the relevant legislation. It is also not uncommon that the documents are in the possession, custody or power of a parent, subsidiary or associated company incorporated or operating in another country. These issues should be brought to the attention of the enforcement agency, which should consider whether assistance could be sought under formal channels from the agency in the foreign jurisdiction, to allow the documents to be produced without violating foreign law.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

There are no blocking statutes as such in Hong Kong. There was some discussion in August 2021 that China's Anti-Foreign Sanctions Law would be introduced into the laws of Hong Kong but that had not happened at the time of writing. It was reported that China's government had decided not to proceed with the plan for the time being.

The jurisdiction to order corporations and individuals to provide evidence in aid of foreign proceedings is derived from Part VIII of the Evidence Ordinance. Section 75 of the Evidence Ordinance requires the application to be made pursuant to a 'request issued by or on behalf of a court' outside Hong Kong. In terms of procedure, therefore, a letter of request is required and Order 70 of the Rules of the High Court provides the procedural framework for taking evidence or obtaining documents from a Hong Kong entity.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Care must be taken to ensure compliance with a company's confidentiality obligations in relation to information. If disclosure to an authority is voluntary, rather than compelled, then the disclosure may violate these obligations.

Law enforcement authorities in Hong Kong must maintain the confidentiality of confidential disclosures made to them (whether voluntary or compelled), except to the extent that they choose to share them with other enforcement authorities, or use the information in an investigation, prosecution or regulatory enforcement action.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies or their directors, officers or employees may face disciplinary action – and disqualification, in the case of directors – and attract potential civil or criminal liability for misconduct in Hong Kong. For entities regulated by the Hong Kong Securities and Futures Commission (SFC), misconduct would include breaches of the Securities and Futures Ordinance (Cap. 571) (SFO), contravention of the terms of any SFC licence or any act prejudicial to the public interest. Sanctions may include a private or public reprimand, a fine of up to HK$10 million or three times the profit gained or loss avoided, revocation or suspension of licences or registrations, and a ban on regulated persons from applying to be licensed or approved as a responsible officer.

The SFC has powers under the SFO to seek criminal prosecution by the Hong Kong Department of Justice (DOJ) and, in practice, the SFC refers all market misconduct cases to the DOJ for advice. The maximum penalties for a person convicted of a market misconduct offence are imprisonment for 10 years and a fine of HK$10 million.

The SFC may also institute civil proceedings before the High Court or the Market Misconduct Tribunal.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

It depends on the laws of the other country in which the corporate wants to settle. The risk of a corporate's suspension, debarment or other restrictions on continuing business in Hong Kong does not, as a matter of Hong Kong law, restrict the corporate from settling in another country; however, there may be legal requirements in that other country (e.g., disclosure obligations) that allow a regulator or law enforcement agency in that country to reopen a settlement if it subsequently discovers the restrictions on the corporate in Hong Kong of which it has not been previously informed.

© Law Business Research 2021

65 What do the authorities in your country take into account when fixing penalties?

The authorities will consider all the circumstances of the case, including (1) the nature and seriousness of the conduct, (2) the value of profits accrued or loss avoided, (3) other circumstances of the firm or individual, and (4) other relevant factors.

In considering the nature and seriousness of market misconduct, the SFC will have regard to the effects of the conduct on market integrity, the costs of the conduct caused to clients or the investing public, the duration and frequency of the conduct, whether there is a breach of fiduciary duty and whether any serious or systematic management or internal control failures are revealed. The SFC will also consider the degree of co-operation with the SFC and other authorities.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

There are no formal mechanisms in Hong Kong for the negotiated settlement of criminal investigations or proceedings that are equivalent to deferred prosecution agreements in the United Kingdom or the United States. However, in some limited circumstances, negotiations with, or representations made to, the Hong Kong Securities and Futures Commission (SFC) and the Hong Kong Department of Justice may result in a decision being taken not to prosecute.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Not applicable.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

The SFC has wide powers to enter into settlement agreements under the Securities and Futures Ordinance (Cap. 571) (SFO) and may do so if this is in the public interest. In considering settlement, aside from considering factors such as the strength of the prosecution and defence cases, the costs and reputational damage of a lengthy investigation and potential subsequent legal proceedings, and possible penalties, institutions should also be aware that the SFC may insist on a public reprimand of the financial institution via an announcement on the SFC's website. The SFC will take into account the degree of co-operation in considering the settlement package.

© Law Business Research 2021

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Not applicable.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

The SFO gives a person who has suffered pecuniary loss as a result of market misconduct the right to bring a civil action to seek compensation. Compensation will only be payable if it is fair, just and reasonable in the circumstances of the case. Findings of the Market Misconduct Tribunal in relation to market misconduct will be admissible as prima facie evidence in the private action, though proceedings before the tribunal are not a prerequisite for bringing civil proceedings. The SFC will not intervene in private legal proceedings.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In practice, law enforcement agencies do not normally publish the commencement of investigations of criminal cases (although they sometimes announce high-profile arrests or dawn raids). Publicity usually follows when a decision has been made to charge an individual or during criminal proceedings once instituted. Criminal trials in Hong Kong are conducted in open court. Some agencies, such as the Hong Kong Securities and Futures Commission and the Independent Commission Against Corruption, publicise the outcome of enforcement proceedings they have initiated on their websites from time to time.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There are no particular factors specific to Hong Kong in managing corporate communications in Hong Kong. The steps are likely to be similar to those that would be taken to manage corporate communications in other jurisdictions, for example, timely, accurate and effective messages using the right media channels, while being sensitive and perceptive to the geopolitical environment. Public relations and media companies can be and have been used in Hong Kong to manage certain corporate crises.

73 How is publicity managed when there are ongoing related proceedings?

Publicity is usually managed by a press officer or communications department that will monitor media reports and suggest the making of public statements as and when necessary. Any public statements made by the company should be carefully drafted and any prejudicial effects on ongoing proceedings should be taken into consideration.

© Law Business Research 2021

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

For a listed corporation, settlement of a regulatory investigation may constitute inside information (depending on the nature and severity of the underlying offence or misconduct) and thus require disclosure as soon as reasonably practicable. In practice, the corporation and the authorities will usually agree on a press release being issued as part of the settlement and will agree on the timing for the release.

By way of context, inside information is defined to include specific information about the corporation that is not generally known to the public but would, if generally known, be likely to materially affect the price of the listed securities. Under Part XIVA of the the Securities and Futures Ordinance (Cap. 571), a listed corporation must, as soon as is reasonably practicable after it becomes aware or is notified of any inside information, disclose the information to the public (subject to certain exceptions).

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

In terms of ESG reporting, there are mandatory disclosure requirements and disclosures required on a 'comply or explain' basis for Hong Kong-listed companies, which were put in place in 2016 and enhanced in 2020.

There are also requirements under the Companies Ordinance that companies registered in Hong Kong include in their annual directors' report a 'discussion' on the company's environmental policies (although there are no clear rules around what that discussion should include).

In April 2019, the Hong Kong Securities and Futures Commission (SFC) introduced high-level disclosure requirements for green and ESG SFC-authorised funds, of which there are now more than 40. Notably, the SFC states that it has obtained 'confirmations and representations' from fund managers but has not independently verified the criteria used to achieve the stated green or ESG investment focuses adopted (in other words, this has been 'light touch' regulation based on what the SFC has been told). This 2019 circular will be superseded on 1 January 2022 by a circular issued on 29 June 2021, which contains requirements in relation to:

- the ESG fund's name;
- offering documents in respect of disclosure of the ESG focus, ESG investment strategy, asset allocation, reference benchmark (such as index fund) and risks or limitations associated with the ESG focus;
- additional disclosure; and
- periodic (at least annual) assessment and disclosure of the attainment of the ESG focus.

© Law Business Research 2021

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

In April 2021, the Stock Exchange of Hong Kong Limited issued a consultation paper on proposed amendments to its Corporate Governance Code, ESG Reporting Guide and Listing Rules to elaborate on the link between corporate governance and the ESG reporting regime, including making clear boards' responsibility for governance and oversight of ESG matters, and assessment and management of ESG risks together with appropriate internal controls. It is also proposed that ESG reports be required to be published at the same time as annual reports effective for the financial year commencing 1 January 2022 (the current requirement is for ESG reports to be published no later than five months after the end of the financial year).

The Fund Manager Code of Conduct is also proposed to be revised to address ESG-related issues; specifically, in October 2020, the SFC issued a consultation paper on Management and Disclosure of Climate-related Risks by Fund Managers, which proposes to introduce requirements that fund managers take climate-related risks into consideration in their investment and risk management processes, make appropriate disclosures to meet investors' growing demand for climate risk information and to combat greenwashing (exaggeration of green credentials).

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

It remains to be seen how, from which regulators and in which sectors we will see enforcement activity, although 'greenwashing' is a stated target. Taking that stated focus, looking back at Hong Kong regulatory enforcement trends in the past decade or so, and extrapolating forward, in the shorter term and given the more mature ESG disclosure requirements for listed companies, enforcement might be expected against listed companies and their directors (1) in respect of false or misleading disclosures inducing share transactions (Securities and Futures Ordinance (Cap. 571) (SFO), section 277) and (2) inside information disclosure failures by listed companies in connection with their ESG reporting (assuming ESG matters are price sensitive for a given company; SFO, Part XIVA). In the medium term, there might be disciplinary action taken by the SFC and other regulators in relation to ESG disclosure failures in respect of their obligations as regulated entities, or breaches of ESG-specific regulatory obligations, for example, in connection with the proposed ESG-related enhancements to the Fund Manager Code of Conduct.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Corporate misconduct, in particular, by listed companies and their directors, will remain a key enforcement priority of the Hong Kong Securities and Futures Commission (SFC), the Independent Commission Against Corruption and the Hong Kong Police Force, as well as the Stock Exchange of Hong Kong Limited (the Exchange). The priorities are to tackle overstatement or embellishing of revenue or financial results and misappropriation

© Law Business Research 2021

of assets. The Exchange has enhanced its disciplinary powers and sanctions, which will have a direct impact on Hong Kong-listed companies and their directors.

In 2020 and 2021, the SFC issued circulars to address misconduct in the context of the operation of bank accounts (June 2021), anti-bribery guidance (December 2020) and leveraged foreign exchange trading activities (April 2020). It launched a consultation in February 2021 to address intermediaries' conduct issues in their carrying out of equity and debt capital raisings in terms of book-building, pricing, allocation and placing activities. In June 2021, consultation conclusions were published for the enhancement of the competency framework for intermediaries, including updating academic and experience entry requirements as well as ongoing competency and training. The revisions are to become effective on 1 January 2022. Another key expected change is the introduction of the investor identification regime (in the second half of 2022) and the over-the-counter securities transactions reporting regime (in the first half of 2023), as indicated in the Consultation Conclusions published in August 2021. This will make the detection of market misconduct more efficient and have a significant effect on enforcement, apart from saving the SFC's time in issuing section 181 notices to firms asking about the information of underlying clients who conduct certain trades.

We also expect closer co-operation between the SFC and the China Securities Regulatory Commission in cross-border investigations, in particular concerning market manipulation in the context of the China–Hong Kong Stock Connect programme, and increased joint operations between enforcement agencies within Hong Kong, apparent from the memoranda of understanding signed between the SFC and the Financial Reporting Council, and between the SFC and the Insurance Authority in 2020 and 2021.

© Law Business Research 2021

15

Ireland

Karen Reynolds, Connor Cassidy and Noel Power[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The investigation into the Irish Bank Resolution Corporation by a Commission of Investigation, connected to the collapse and subsequent winding down of Anglo Irish Bank plc, remains the highest-profile current corporate investigation in Ireland. When it was established, 38 transactions were within focus of the investigation. The related trial of certain high-ranking banking executives concerning their conduct before the collapse was the longest criminal trial in the history of the state and resulted in penal sentences, which are rarely imposed in Irish business crime cases. This investigation is one of the most complex ever to have been carried out by the Garda National Economic Crime Bureau (GNECB) and concerns allegations of a €7.2 billion conspiracy to defraud. In July 2021, the Commission of Investigation finalised its draft report in respect of just one of the 38 transactions: the sale of Siteserv to businessman Denis O'Brien at the height of the financial crisis. It is unlikely that the final report will be published before 2022.

The Office of the Director of Corporate Enforcement (ODCE) launched a high-profile investigation into Independent News and Media plc (INM). In September 2018, the president of the High Court granted an application by the ODCE to appoint inspectors to INM and investigate whether there may have been alleged unlawful sharing of the company's information.

The approach in relation to the INM investigation was the first brought under section 748 of the Companies Act 2014, which is a relatively new provision. The judgment, therefore, provides guidance on the scope of the powers of the High Court. The Court

1 Karen Reynolds is a partner and Connor Cassidy and Noel Power are senior associates at Matheson.

© Law Business Research 2021

held that the existence of other statutory investigations into the same subject matter of an application does not automatically preclude the appointment of inspectors and the Court will engage in an assessment of the adequacy of those investigations to deal with the issues raised in an application, taking into account matters such as the nature of the powers available to the statutory bodies in question, their power to publish a report, and the effect and status of such a report. In February 2021, the High Court dismissed an application made by the former chairman of INM, Leslie Buckley, to remove two of the appointed inspectors on the grounds of objective bias.

The judgment also brings renewed focus to the role of the ODCE and its ability to carry out its enforcement functions effectually. The government, in its Package on White Collar Crime announced in November 2017, committed to re-establish the ODCE as a new independent agency in an effort to enhance the state's corporate law enforcement capacity. In that regard, in September 2021, the government published the Companies (Corporate Enforcement Authority) Bill 2021. The Bill provides for the establishment of the ODCE as a statutory, stand-alone agency charged, with the Corporate Enforcement Authority (CEA), with increased autonomy and resources to respond to white-collar crime in Ireland. Although the Bill continues to progress at governmental level, the transition is already under way.

The ODCE has faced challenges, particularly regarding the pace of progression of investigations. White-collar crime investigations are typically complex and can take several years to complete. For example, the former charity Console was referred to the Director of Public Prosecutions (DPP) in May 2019. A pretrial hearing has been scheduled for 2022, with the trial itself scheduled for January 2023. In this context, the enactment of the Criminal Procedure Act 2021 should be a welcome development (once commenced), the primary purpose of which is to provide for pretrial hearings, which should reduce delays in complex economic crime prosecutions.

2 Outline the legal framework for corporate liability in your country.

Corporations are separate legal entities and a company can be found liable for the criminal acts of its officers. Companies can be vicariously liable for the conduct of employees. When the doctrine of vicarious liability does not apply, the state of mind of an employee can be attributed to the company in circumstances in which the human agent is the 'directing mind and will' of the company, or when an individual's conduct can be attributed to the company under the particular rule under construction. A company can also be guilty of a strict liability offence, which is an offence that does not require any natural person to have acted with a guilty mind, such as health and safety legislation infringements. The Criminal Justice (Corruption Offences) Act 2018 has also created a strict liability offence for companies in respect of corruption and bribery offences. Under section 18 of this Act, a corporate body can be guilty of a criminal offence if one of its officers, employees, agents, subsidiaries or persons purporting to act as such commits a corruption offence with the intention of obtaining or retaining business or an advantage for the company. The corporate has a defence if it can show that it took all reasonable steps and exercised due diligence.

© Law Business Research 2021

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

An Garda Síochána is the primary body with responsibility for the investigation and prosecution of crime in Ireland, with a specialist wing for complex economic crimes (the GNECB). Other law enforcement agencies, or regulators, with a focus on corporate offences and business crimes are as follows:

- the ODCE, which will soon be replaced by the CEA, monitors and prosecutes violations of company law;
- the Office of the Revenue Commissioners is responsible for the collection, monitoring and enforcement of tax laws;
- the Competition and Consumer Protection Commission (CCPC) is responsible for competition law and consumer protection;
- the Central Bank of Ireland (CBI) regulates financial institutions;
- the Health and Safety Authority enforces occupational health and safety law; and
- the Data Protection Commission (DPC) is responsible for data protection law.

Generally, regulatory bodies are empowered to prosecute only (some) summary (minor) offences. The Office of the DPP is responsible for prosecuting criminal offences on indictment (serious) and summary offences. The DPP has no investigative functions. Cases are referred by the relevant investigatory body.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

This will depend on the statutory basis for the investigation. For the most part, investigations are initiated on the basis of a complaint alleging that an offence has been committed. Some bodies can only initiate investigations following receipt of a complaint alleging that an offence has been committed, whereas others, such as the GNECB, the CBI and the DPC, can initiate investigations on their own initiative. Different factors and thresholds are relied on by different bodies. The GNECB relies on a variety of factors, such as monetary loss, the international or cross-border significance and the complexity of the issues of law or procedure that arise. In 2020, the ODCE received 149 complaints and directed 55 criminal charges against named individuals for offences including fraudulent trading, theft and money laundering.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A challenge could be initiated in the Irish courts through judicial review proceedings. Sometimes a compromise can be reached with the law enforcement agency on the scope of the notice. In certain circumstances it may be possible to get an interim injunction preventing the exercise of the notice, subpoena or warrant, or preventing the authority from using information already obtained, unless and until the court determines that the validity of the instrument is valid and enforceable.

© Law Business Research 2021

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Irish law does not recognise plea bargaining or co-operative agreements. The decision to prosecute is at the discretion of the DPP and the courts have discretion in imposing sentences within the statutory minimum and maximum periods.

7 What are the top priorities for your country's law enforcement authorities?

The Irish government has a renewed focus on tackling white-collar crime, particularly following the publication of the Hamilton Report in December 2020. The government also recently passed the Criminal Procedure Act 2021 into law, which should provide efficiencies in the trial process.

In its Annual Report for 2020, the ODCE has indicated that it expects to see an increase in the number of directors' restriction and disqualification undertakings being issued. It also expected that a number of its investigations would result in files being submitted to the DPP for consideration later in 2021. The ODCE observed a reduction in auditors' reports and complaints from the public in 2020 and anticipated that this trend would reverse in 2021, which in turn will give rise to associated enforcement activities.

The CBI's enforcement priorities for 2021 include, among other things, taking enforcement action where it sees serious instances of consumer or investor harm from the behaviour or failings of firms and individuals, reforming the fitness and probity regime and individual accountability (with the General Scheme for the Central Bank (Individual Accountability Framework) Bill having been published in July 2021), the behaviour and culture of regulated entities, money laundering and counter-terrorism financing compliance.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

It is vital for corporations to be seen to have an effective regulatory compliance and corporate governance programme. Under section 225 of the Companies Act 2014, company directors are required to include in their annual report a statement to confirm (1) the company's policies in respect of compliance by the company with its relevant obligations under company law and tax law, (2) the putting in place of appropriate structures designed to secure material compliance with these obligations, and (3) that a review of the structures has taken place during the previous financial year. In addition, specific legislation imposes further obligations, such as the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). Under the GDPR, companies are required to establish a data protection compliance programme informed by GDPR principles, including the appointment of a data protection officer, providing training to employees and conducting internal data audits and compliance reviews.

© Law Business Research 2021

In terms of what constitutes an effective compliance programme, section 225 of the Companies Act 2014 provides that the structures put in place 'shall be regarded as being designed to secure material compliance' if these structures 'provide a reasonable assurance of compliance in all material respects with those obligations'.

The Department of Finance published information on its own corporate governance framework in October 2019. This publication contains some commentary on what constitutes an effective governance framework. It noted that good corporate governance 'provides clarity in relation to authority and responsibility, it supports effective decision-making and it identifies the assurance and accountability arrangements that exist within any organisation'.

The Corruption Offences Act 2018 provides corporates with a defence to the corporate liability offence under the Act if they can show that they took all reasonable steps and exercised due diligence to avoid the commission of the offence.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 impose requirements on operators of essential services (OESs) and digital service providers (DSPs) to manage the risks to the security of network and information systems. OESs include operators within specified sectors, including energy, transport, banking, financial market infrastructure, health and digital infrastructure. DSPs are those who provide digital services, including online marketplaces, online search engines and cloud computing services. There is a centralised computer security incident response team in the Department of Communications, Climate Action and the Environment, which both OESs and DSPs must notify if there are incidents that have a significant or substantial impact on these services. The Central Bank of Ireland also takes enforcement action against any financial service provider whose failings in cybersecurity cause it to breach its regulatory requirements.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Criminal Justice (Offences Relating to Information Systems) Act 2017 was the first Irish legislation to specifically address the issue of cybercrime. The Criminal Justice (Theft and Fraud Offences) Act 2001 also provides that it is an offence to use a computer with the dishonest intention of causing a loss to another person. An Garda Síochána has a specialist division (the Garda National Cyber Crime Bureau) that investigates cybercrime.

In 2021, the Irish Health Service Executive was the victim of a serious ransomware attack. The investigation into the attack continues to be led by the Garda in collaboration with international law enforcement agencies, including Interpol and Europol.

© Law Business Research 2021

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Ireland is bound by the EU's European Arrest Warrant Framework Decision, as implemented in Ireland by the European Arrest Warrant Act 2003, under which arrest and extradition is coordinated among EU Member States. Legal assistance can be requested and provided by Irish authorities to law enforcement in other jurisdictions under the Criminal Justice (Mutual Assistance) Acts 2008 and 2015. However, Ireland will only allow extradition in circumstances where (1) a person has been charged with an offence (i.e., not for the purpose of merely investigating a criminal offence), (2) the offence is not a political offence, and (3) the offence does not carry the death penalty.

Other examples of extraterritorial jurisdiction are set out below.

Corruption

The Criminal Justice (Corruption Offences) Act 2018 prohibits bribery offences occurring outside Ireland in two sets of circumstances: (1) if an Irish person or company does something outside Ireland that, if done within Ireland, would constitute an offence under the corruption legislation, that person is liable as if the offence had been committed in Ireland; and (2) if an offence under the corruption legislation takes place partly in Ireland and partly in a foreign jurisdiction, a person may be tried in Ireland for that offence. There is no requirement that the offending act should also be an offence in the foreign jurisdiction where the offending act took place.

Money laundering

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (the CJ(MLTF) Act) sets out specific circumstances in which an action can be taken for money laundering occurring outside Ireland. If an individual or a company engages in conduct in a foreign jurisdiction that would constitute a money laundering offence both under the CJ(MLTF) Act and in that foreign jurisdiction, they can be prosecuted in Ireland. This extraterritorial jurisdiction may be exercised only if the individual is an Irish citizen, ordinarily resident in the state, or the body corporate is established by the state or registered under the Companies Act 2014.

Proceeds of crime

Under the Proceeds of Crime Act 2016, the Irish High Court can make orders depriving a defendant of assets that are merely suspected of being the proceeds of crime, regardless of whether the defendant has been convicted of a criminal offence. 'Proceeds of crime' for the purposes of the Act means any property obtained or received at any time by, or as a result of, or in connection with criminal conduct. The definition of 'criminal conduct' is such that foreign criminality is covered by the scope of the act where the proceeds are within the state.

© Law Business Research 2021

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

For investigations by Irish regulators and law enforcement agencies, the foremost consideration will be whether there is an existing framework for co-operation between Ireland and the other jurisdiction (or jurisdictions). The Criminal Justice (Mutual Assistance) Act 2008, as amended, gives effect to international agreements that establish the existing legislative framework for the provision of mutual legal assistance.

Investigations by regulators or law enforcement and by corporations can also encounter difficulties owing to different legal standards. For example, data protection laws in some countries can restrict the flow of information out of the country, and different levels of protection for private data may restrict the possibility of transfer between the jurisdictions. Further, different rules can apply to matters such as the application of privilege and the constitutional protections owed to persons under investigation.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

A corporation cannot be prosecuted twice for the same or similar offences on the same facts following a legitimate acquittal or conviction by an Irish court or by a court of competent authority in a foreign jurisdiction. There must be identity between the foreign and domestic offences.

Typically, the principle does not apply until proceedings are concluded. However, under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended), no proceedings may be initiated in circumstances where an individual has been charged under that Act in the absence of consent from the Director of Public Prosecutions.

There is no anti-piling on policy in Ireland that prevents multiple enforcement authorities from taking action against an entity in relation to the same conduct.

14 Are 'global' settlements common in your country? What are the practical considerations?

It is possible for a domestic authority to reach a resolution as part of a coordinated approach with an overseas authority. However, if a party wishes to reach a settlement with authorities in another country or countries, it should be aware that such an agreement may not prevent Irish authorities from continuing to pursue a prosecution.

© Law Business Research 2021

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Investigations into similar matters in other jurisdictions are often the catalyst for investigations in Ireland. Irish authorities will usually try, and in certain instances may be obliged, to co-operate with foreign investigation authorities, and the exchange of information through appropriate channels can aid an investigation greatly. Ultimately, it will be a matter for the Irish authorities to determine whether and how to conduct their own investigations.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Sanctions imposed at an international level are implemented at a national level. Therefore, individuals and companies operating in Ireland should be aware of the restrictions imposed under Irish law that implement international sanctions. As a Member State of both the United Nations and the European Union, Ireland is required to observe and enforce UN Security Council sanctions and EU restrictive measures. The Department of Foreign Affairs and Trade, the Department of Business, Enterprise and Innovation and the Central Bank of Ireland (CBI) are the competent authorities in Ireland and they will enforce sanctions imposed by either the European Union or the United Nations.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Any regulated entity in Ireland could find itself subject to enforcement action in respect of policies and procedures around financial sanctions screening.

Sanctions enforcement activity has increased on account of the European Union being more proactive in imposing sanctions. There have been no enforcement settlements issued by the CBI to date specifically in respect of failures concerning a firm's financial sanctions screening process.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Yes. Sanctions imposed at an international level are implemented at a national level. The Department of Foreign Affairs and Trade, the Department of Business, Enterprise and Innovation and the CBI will work with their counterparts in other jurisdictions to enforce sanctions imposed by either the European Union or the United Nations.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

As a member of the European Union, Ireland is subject to the EU Blocking Regulation. The Regulation effectively nullifies the extraterritorial application of the US sanctions against Iran by (1) prohibiting compliance with any sanctions imposed by the United States, (2) preventing the enforcement of any judgment from a foreign court outside the European Union that gives effect to the sanctions, (3) requiring any EU person, natural or legal, to notify the European Commission of any effects that the sanctions may have on them, and (4) allowing any EU person to seek compensation caused by the application of the sanctions.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

The Irish courts implement certain aspects of the EU Blocking Regulation by not enforcing or recognising any judgments that may be made outside the European Union. Further, the courts will allow EU persons to seek compensation in the Irish court system for any adverse effects caused by the application of US sanctions.

Under SI 217/1997 (European Communities (Extraterritorial Application of Legislation Adopted By a Third Country) Regulations), failure to comply with the EU Blocking Regulation is an offence and may be punished by a fine or up to 12 months' imprisonment.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct will often be raised by whistleblowers, who are protected by the Protected Disclosures Act 2014. Accordingly, great care must be taken not to violate these protections when allegations come to light in this way. Under the Central Bank (Supervision and Enforcement) Act 2013, there are specific whistleblower protections in relation to making disclosures to the Central Bank of Ireland (CBI) when breaches of financial services legislation may be in issue.

Thematic reviews are typically carried out by regulators. For example, the CBI often bases its investigations on the Administrative Sanction Procedure under the Central Bank Act 1942 (as amended) on matters identified during thematic reviews.

Allegations of misconduct also come to light following complaints from members of the public. For example, in 2020, the Office of the Director of Corporate Enforcement received 149 complaints and the CBI received 15 formal complaints from members of the public.

When allegations arise through media reports, publicised litigation or other publicised external sources, there are more immediate public relations risks than when a matter arises internally.

© Law Business Research 2021

There are specific legislative provisions that oblige persons to report information in relation to certain offences in certain circumstances. The Supreme Court upheld the enforceability of section 19 of the Criminal Justice Act 2011 (which sets out the offence of 'withholding information' and involves a mandatory reporting obligation in specific circumstances) in *Sweeney v. Ireland* [2019] IESC 39. If a company is a regulated entity, it may be required to make certain disclosures to its regulator, or indeed to self-report unintentional breaches or offences. Auditors have disclosure obligations, and misconduct coming to light during their engagement may trigger a reporting obligation. In early 2021, the European Court of Justice in *DB v. Commissione Nazionale per la Società e la Borsa* (Case C-481/19) confirmed that natural persons have the right to silence under EU law, particularly in administrative proceedings of a criminal nature. The implications of this judgment are potentially relevant in a number of Irish regulatory contexts, including under the CBI's Administrative Sanction Procedure and the Competition and Consumer Protection Commission's enforcement regime.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Ireland's data protection regime mainly comprises the EU General Data Protection Regulation (GDPR) and the Data Protection Acts 1988–2018 (the DP Acts). Within this regime, data controllers have a number of duties, including an obligation to process personal data (under the meaning of the GDPR and the DP Acts) fairly, for it to be kept up to date and secure.

Additionally, the Criminal Justice (Offences Relating to Information Systems) Act 2017 gives effect to provisions of Directive 2013/40/EU on attacks against information systems, which introduced a number of criminal offences.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Data Protection Commission (DPC) is responsible for monitoring the application of the DP Acts and the GDPR to protect the rights and freedoms of individuals in relation to processing.

The DPC has a number of investigative powers, including the power to conduct an audit, the power to compel individuals and companies to provide it with information and documentation, and the power to prohibit the transfer of personal data overseas.

Summary proceedings may be brought and prosecuted by the DPC. In relation to indictable offences, the DPC prepares a file and submits it to the Director of Public Prosecutions for consideration.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The GDPR and the DP Acts restrict the use and disclosure of an individual's data in Ireland. There are exceptions to the protection given under the DP Acts, but there is

© Law Business Research 2021

no specific exemption when an internal investigation is being carried out. Traditionally, companies have relied on consent to support internal investigations; however, the DP Acts now require that consent be freely given to be valid. The GDPR requires that a data subject can withdraw his or her consent at any time. These factors make it difficult for employers, in the majority of circumstances, to rely on consent as a legal basis for processing data, albeit not impossible.

Companies should therefore seek an alternative lawful basis for processing in the context of internal investigations. The DP Acts allow for data to be processed if it is necessary for the purposes of legitimate interests pursued by the data controller, which can be the case for an internal investigation, but that needs to be balanced against the fundamental rights and freedoms and the legitimate interests of the data subject in question.

Irish law recognises a broad 'right to privacy', which includes a right to privacy at work, and a person does not lose privacy and data protection rights simply by being an employee. Any limitation of an employee's right to privacy should be proportionate to the likely damage to the employer's legitimate interests.

If an employer seeks to use 'legitimate interests' as the basis for processing data, an employee as data subject will have a right to object to that processing of their data. This right is not absolute and may be overridden by the employer having 'compelling reasons' to process the data. Companies must inform their employees of the right to object and should draft an internal investigation policy reflecting this balance. Employees should be notified of the possibility that an investigation might take place and, in particular, the ways in which their personal data might be processed in the context of an investigation. For new employees, this information should be provided when they join the company. However, for existing employees, the provision of an updated internal investigation policy will be sufficient.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Irish employers have the right to monitor employees' communications. However, this is subject to the right to privacy that employees are afforded under both the Irish Constitution and the European Convention on Human Rights, as well as under data protection law. Any intrusion of an employee's right to privacy must be proportionate to any likely damage caused to the employer's legitimate interests.

When an employee wishes to enforce the right to privacy or believes that it has been infringed, he or she may do so by referring a dispute to the Workplace Relations Commission or by commencing proceedings in the courts. If the dispute involves an employee's personal data, it may be possible to lodge a complaint with the DPC.

© Law Business Research 2021

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and dawn raids are often used as part of investigations against companies, particularly by the Competition and Consumer Protection Commission and the Office of the Director of Corporate Enforcement. Both company premises and private homes of relevant persons can be searched on the basis of an appropriate warrant.

There are constitutional protections for persons subject to searches, particularly of private homes. Depending on the specific statute, a regulator or investigatory body would obtain a search warrant to enter a dwelling to conduct a search and to seize documents. There is a general requirement that there is some nexus between the investigation by the regulatory body of the offence in question and the dwelling in question. The body is only permitted to search the premises specified in the warrant and to seize items included within the terms of the warrant.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privileged material is prima facie protected from examination by law enforcement or regulatory bodies. Specific statutes, such as the Companies Act 2014 and the Central Bank (Supervision and Enforcement) Act 2013, also provide for the protection of privileged information during investigations.

In practical terms, it can be difficult to determine during a seizure operation whether material is privileged, and sometimes the material will be isolated so that a claim of privilege can be assessed later.

The mechanism to assess whether privilege has been properly asserted will be dependent on the legislation under which the search warrant was granted.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The Irish Constitution recognises a right to silence and the privilege against self-incrimination. Arrested suspects are brought into police custody for questioning 'under caution'. The suspects should be cautioned that they have the right to maintain silence and that anything they say may be used in evidence. However, the Criminal Justice Act 1984 (as amended) provides that, in the case of arrestable offences (i.e., those for which a person can be imprisoned for five years or more), inferences can be drawn at trial from an accused's silence.

The right to silence can be abridged by statute, most often in the context of regulatory investigations, meaning that answers can be compelled. However, Irish courts have frequently held that statements given under statutory compulsion (such as in connection

© Law Business Research 2021

with a regulatory investigation attracting a civil penalty) cannot be used against that person in subsequent criminal proceedings, whereas voluntary statements can.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Protected Disclosures Act 2014 (the 2014 Act) protects whistleblowers and provides for a tiered disclosure regime with a number of avenues open to whistleblowers. The 2014 Act encourages the vast majority of protected disclosures to be made to the employer in the first instance. However, other options are available if this is inappropriate or impossible.

When a worker makes a protected disclosure, the employer in question is prevented from dismissing or penalising the worker, taking an action for damages or an action arising under criminal law, or disclosing any information that might identify the person who made the disclosure. If the employer were to dismiss or penalise a worker wholly or mainly as a result of him or her making a protected disclosure, the worker could be awarded up to five years' remuneration, re-engagement or reinstatement by the Workplace Relations Commission (the employment tribunal in Ireland). Further, the 2014 Act creates a cause of action in tort for the worker for detriment suffered as a result of making a protected disclosure. The General Scheme of the Protected Disclosures (Amendment) Bill was published in May 2021 following approval by government. The purpose of the Bill is to provide for the transposition of the EU Whistleblowing Directive into Irish law. Ireland is one of just 10 EU Member States to already have comprehensive legal protections for whistleblowers.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

As a general matter, employees have a constitutional right to 'fair procedures' in any investigative or disciplinary process. This means that, among other things, an employee must be kept apprised of the investigation and must be permitted to participate in the investigation, test the evidence and make points in his or her defence. The extent and scope of fair procedures and natural justice that must be afforded during a workplace investigation depends on the actual nature of the investigation and the potential consequences thereof.

The rights do not differ for officers and directors who are employees.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Constitutional rights apply in an investigation and disciplinary process when a person is implicated or suspected of having engaged in misconduct.

Prior to a finding of misconduct being made, an investigation and disciplinary process should be carried out.

The disciplinary process should, at a minimum, follow the Workplace Relations Commission's Code of Practice on Disciplinary and Grievance Procedures and the employer's own procedures, and involve the following basic principles:

- Advance written notice of any allegations, and any supporting documentation and witness statements, should be provided to the employee.
- The employee should be invited, in writing, to an investigation meeting to discuss the allegations and to put forward his or her response.
- The investigation should go no further than to determine whether there is a sufficient factual basis to warrant a matter being put to a disciplinary hearing.
- Suspension should be imposed only after full consideration of the necessity for it pending a full investigation of matters. It may be justified if it is to prevent repetition of the conduct complained of or interference with evidence; to protect individuals at risk from such conduct; to comply with any regulatory rule applicable to the individual or their role; or to protect the employer's business and reputation. Suspension must be on full pay and benefits, and for no longer than is reasonably necessary.
- Depending on the outcome of an investigation, the employee should be invited in writing to a disciplinary meeting to discuss the allegations and to put forward a response. Documents obtained during the investigation should be provided to the employee.
- The employee should be allowed to be accompanied by a colleague or trade union representative at any meetings.
- Any sanction must be proportionate and reasonable in the circumstances and should be confirmed in writing to the employee.
- A right of appeal to someone not previously involved should be provided.
- Unless the allegations are sufficient to constitute gross misconduct, the sanctions should progress from verbal warning to written warning to final written warning and then to dismissal. Summary dismissal will be permitted only when the circumstances genuinely constitute gross misconduct.

For dismissal for out-of-work misconduct to be deemed fair, there must be a genuine connection between the employee's offence and his or her employment. The connection must be such that it leads to a breach of trust or causes reputational or other damage to the employer. In these circumstances, the employer should carry out its own internal investigation and disciplinary process (in accordance with the requirements set out above).

© Law Business Research 2021

32 Can an employee be dismissed for refusing to participate in an internal investigation?

The extent to which an employer may take disciplinary action against an employee for failure to participate in an investigation will depend on the circumstances.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

There is no statutory requirement for such a document, but it would be considered general good practice. Depending on the circumstances, it may be useful to detail the purpose and scope of the investigation and to clarify the remit of the investigators' role. Matters to cover might include:

- the structure and methodology of the investigation;
- a definition of the issues to be covered; and
- details of any engagement with legal counsel and related matters concerning privileged material.

If the investigation concerns employees of the company, it should go no further than gathering the relevant information or evidence to determine whether there is a sufficient factual basis to put particular allegations at a formal disciplinary hearing. The investigation should be carried out in accordance with any relevant internal procedures and not reach any factual conclusions on the evidence or decide whether the allegations are proved.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Depending on the severity of the issue, it would usually be prudent for a business to carry out a certain level of enquiry and investigation. However, a company should take care in carrying out any investigations and in creating any reports, as it is possible that any such documents could be subject to disclosure in subsequent legal proceedings. A company would not generally be obliged to voluntarily provide the results of such an investigation to the relevant authorities unless it is required under a court order or statute, or as part of a self-report. A number of legislative provisions impose a positive obligation on persons (including businesses) to report wrongdoing in certain circumstances (e.g., section 19 of the Criminal Justice Act 2011).

It is also essential that any wrongdoing ceases as soon as the company becomes aware of it, and that remedial measures are taken where appropriate. Care should be taken to preserve evidence of the wrongdoing, as a failure to do so could result in accusations of destruction of evidence, which can itself be an offence under certain legislation.

© Law Business Research 2021

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is advisable to immediately implement a 'document hold' by suspending deletion policies and circulating document retention notices.

The company should review the request and consider the power under which it is exercised, and in particular if the request is voluntary or mandatory. There are risks associated with releasing documentation, particularly when it might contain confidential or personal information, without being lawfully compelled to do so. External legal advice may be required in this regard.

An inventory listing the materials falling within the notice should also be prepared. The material should then be assessed for privilege. Copies of anything provided to the investigation authority should be retained.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement. There may, of course, be commercial reasons for doing so (or not doing so) in any particular case.

Under the Irish Listing Rules, publicly listed companies on the Irish Stock Exchange (Euronext Dublin) must, without delay, provide to Euronext Dublin any information that it considers appropriate to protect investors. Euronext Dublin may, at any time, require an issuer to publish such information within the time limits as it considers appropriate to protect investors or to ensure the smooth operation of the market.

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are considered part of good corporate governance. However, companies operating in Ireland can be subject to certain reporting obligations in respect of certain offences and will therefore be required to notify matters to law enforcement or regulators in certain circumstances. For example, persons with a 'pre-approved control function' are required to report breaches of financial services legislation and designated persons (including auditors, financial institutions and solicitors) have an obligation to report money laundering offences.

However, if criminal prosecution precedes an internal investigation, in general, internal disciplinary procedures are suspended to respect the individual's right to silence.

© Law Business Research 2021

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Any requirement to disclose documents obtained through an internal investigation to the Irish authorities is qualified by legal professional privilege. There are two forms of legal professional privilege in Ireland:

- legal advice privilege, which applies to confidential communications between a lawyer and a client that are created for the sole or dominant purpose of giving or seeking legal advice; and
- litigation privilege, which applies to communications between a lawyer and a client made in the context of contemplated or existing litigation or regulatory action. It also covers communications with third parties, such as experts.

Litigation privilege is a broader form of privilege to assert in the context of an internal investigation, provided there is actual or contemplated litigation or regulatory action.

The main way to protect and preserve privilege is to involve lawyers in internal investigations at an early stage, although it should be noted that privilege cannot be asserted in respect of pre-existing documents after they have been created merely by involving lawyers. To ensure that existing privilege is not lost, it is important to limit the disclosure or sharing of privileged materials to only those persons who are authorised to seek or receive the privileged material. Legal advice should not be summarised or copied and shared by non-legal persons. If privileged materials need to be shared with third parties, it is important to ensure that appropriate confidentiality agreements are put in place to govern the disclosure to ensure that, as far as possible, privilege is not inadvertently waived or lost.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal professional privilege applies equally to individuals and companies and can only be waived by the client. Under Irish law, the question of who is the client in a corporate context was considered in *UCC v. ESB [2014] IEHC 135*, where it was held that if the client is a corporate body, it is necessary to consider whether the individual making the communication to the lawyer is a person engaged or employed to obtain or receive legal advice on behalf of the client.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, subject to the criteria for legal professional privilege being met. In-house counsel must be acting in his or her capacity as legal adviser and not as an officer of the company. However, the position with regard to in-house counsel in the context of certain external matters is not straightforward and advice should be sought as a result of the decision of

© Law Business Research 2021

the European Court of Justice in *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. Commission* (Case C-550/07 P).

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The definition of 'lawyer' in Ireland extends to foreign lawyers. There does not appear to be any question about this and it is generally accepted that foreign legal advice is privileged to the extent that it fits Irish legal rules on privilege.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Asserting legal professional privilege is a fundamental legal right and the fact of its assertion should not be held against a party. However, if the materials over which legal professional privilege is being asserted are central to any enforcement investigation (such as a party defending certain conduct on the basis that it was taken following legal advice), it may appear unco-operative to refuse to disclose those materials. In such a case, disclosure could, in fact, be in a party's strategic interest. Any decision to waive privilege should be carefully considered as, once waived, legal professional privilege is lost. It is generally recommended that a waiver should be limited to those materials that are strictly necessary and should be made on a limited and specified basis; in other words, a general waiver of all legal professional privilege in respect of a particular matter is not advisable.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

It is possible to waive privilege on a limited basis. However, care should be taken as privilege can inadvertently be lost in such circumstances. The scope of the waiver should be clear, limited and in writing; furthermore, it is of utmost importance that confidentiality in the material should be maintained. Care should be taken when waiving privilege over documents that make reference to connected documents over which privilege is maintained. The Irish courts do not permit parties to 'cherry-pick' which privileged information they wish to disclose. In *Quinn v. IBRC* [2018] IEHC 481, the court held that, in certain circumstances, a partial disclosure of privileged documents may create an unfair litigious advantage if a litigant retains privilege over other connected documents. Therefore, a partial disclosure can result in a wider waiver of privilege.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If the waiver of privilege was appropriate, limited and restricted, it should not defeat the overall assertion of legal professional privilege. However, this will depend on the extent and nature of the waiver in each case.

© Law Business Research 2021

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in Ireland. It is important that common interest privilege is expressly asserted and that the receiving third party is aware of the necessity of preserving privilege in the materials received.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Litigation privilege can be asserted regarding third-party communications where the dominant purpose of the communication is in anticipation of existing or contemplated litigation (which currently includes regulatory proceedings).

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, and this is often an integral part of the fact-finding exercise of an investigation. However, the internal investigation would not be able to compel witnesses to attend, except to the extent that employees can be requested to co-operate in the context of their employment.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes, where reports contain legal analysis, advice or conclusions, or are prepared with the dominant purpose of preparing for, or in contemplation of or in connection with, litigation or regulatory proceedings.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

It can be important that witnesses are informed of the nature of the interview, whether they are implicated in any wrongdoing and, crucially, of any possible consequences for them of the investigation process to preserve the ability to take appropriate action, if necessary, following or as a result of the investigation. It is important to point out that any lawyers present are acting for the company and not for the employee, who may, in some cases, have his or her own legal representation.

Existing employees have a greater right to fair procedures as they are more likely to face the possibility of an adverse outcome, such as dismissal. However, it is best practice to accord equal and fair procedures to all interviewees.

© Law Business Research 2021

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

It is good practice to ensure that any documents of relevance to the witness are put to them. 'Interview by ambush' is contrary to fair procedures and open to challenge, particularly by employees.

Employees have no statutory right to legal representation at witness interviews. However, if the employee or witness is, or may become, the subject of the investigation, the employer should consider advising the employee or witness to have legal representation to minimise the risk of a later legal challenge to the investigation process. If the person requests permission to have legal representation, the company should assess each case separately. It is generally considered prudent to permit such representation, or not to proceed in the absence of such representation.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

A number of legislative provisions impose a positive obligation on persons (including businesses) to report wrongdoing in certain circumstances. Most significantly, section 19 of the Criminal Justice Act 2011 provides that a person is guilty of an offence if he or she fails to report information that he or she knows or believes might be of 'material assistance' in preventing the commission of, or securing the prosecution of another person in respect of, certain listed offences, including many corporate crimes. The disclosure must be made 'as soon as practicable', and a person who fails to disclose such information may be liable to a fine or imprisonment for up to five years, or both. However, the person considering making the report may need to make enquiries to be satisfied that a report is justified.

Other mandatory reporting obligations include the duties of:

- persons with a 'pre-approved control function' to report breaches of financial services legislation;
- designated persons (such as auditors, financial institutions and solicitors) to report money laundering offences;
- auditors to report a belief that an indictable offence has been committed;
- auditors or persons preparing accounts to report theft and fraud offences; and
- all persons to report any offence committed against a child.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

A company might be advised to self-report, in Ireland or overseas, to mitigate the risk of prosecution or any potential sentence that may be imposed by a court. There are no express provisions for immunity or leniency in prosecution under Irish law, but self-reporting can be considered a mitigating factor in sentencing. The Director of Public Prosecutions does

© Law Business Research 2021

have discretion to grant immunity in certain circumstances. Some regulatory regimes, such as the Central Bank of Ireland's (CBI) administrative sanction procedure, also consider self-reporting as a mitigating factor affecting the level of sanctions. The list of sanctioning factors set out in the CBI's Administrative Sanctions Procedure (published in 2018) includes 'how quickly, effectively and completely the regulated entity brought the contravention to the attention of the CBI or any other relevant regulatory body'.

The exception is the Cartel Immunity Programme operated by the Competition and Consumer Protection Commission (CCPC), which allows a member of a cartel to apply for immunity in return for co-operating with the CCPC. Only the first member of a cartel to come forward can avail of the programme and must meet strict eligibility criteria.

In terms of extraterritorial self-reporting, an Irish company may self-report to authorities in other jurisdictions that have immunity or leniency programmes if the conduct in question could also be investigated or prosecuted by those authorities.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

It is important that a company has considered its risks and, as far as possible, investigated the matter before making a report. A report can be made in writing, such as by letter to the appropriate authority, or by providing a written statement when attending a Garda station. The form and content of the report will depend on the specific circumstances of the matter, including, for example, whether the company might be implicated, or whether there are other legal, commercial or reputational issues to be considered. Data deletion policies should be suspended and relevant materials retained in case they are subsequently required in the context of an investigation or legal or regulatory proceedings.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Dialogue may start with the authority once a notice has been received and analysed. For example, the company may wish to address concerns such as the scope of the request, the legal basis or the deadline for compliance. It is important that care is taken with these types of communications, as they can set the tone for engagement with the authority and may be relevant for any subsequent court challenge or dispute that may arise.

55 Are ongoing authority investigations subject to challenge before the courts?

Yes, for example, through an application for judicial review. It is also possible to seek injunctions, typically on an interim basis, to protect legal rights while the underlying challenge is resolved.

© Law Business Research 2021

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Each request should be treated separately as the legal basis for the request is likely to be different. A request that may appear to compel disclosure of documents may not, in fact, have legal effect if it is from outside the jurisdiction and the procedures for compelling cross-border information (such as the procedures under the Criminal Justice (Mutual Assistance) Act 2008, as amended) are not engaged. It is generally not advisable to release information, in the absence of lawful compulsion. 'Package disclosures' are therefore usually inadvisable, as documents that one agency has a legal right to obtain may not be within the compulsory power of another agency. That said, when requests are made by different authorities, it is important to have a consistent approach with regard to how requests are treated and what arguments are made to authorities.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The appropriate response will depend on the nature of the request and the relationship between the company that is subject to the request and the entities holding the documents across borders. If the company in receipt of the request has the power to compel production, such as from a branch or subsidiary, it may be required to do so. However, generally, the entity to which the request is addressed will be the only body with an obligation to respond.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

In terms of formal co-operation mechanisms, the Criminal Justice (Mutual Assistance) Act 2008 gives effect to 12 international agreements that establish the existing legislative framework for the provision of mutual legal assistance. The Criminal Justice (Mutual Assistance) (Amendment) Act 2015 gives effect to a further six international instruments not provided for by the 2008 Act. This has enhanced the already significant level of co-operation between Ireland and other EU Member States. Co-operation with third countries (those outside the European Economic Area) is dependent on their ratification of relevant international agreements or the existence of a mutual assistance treaty agreed between them.

The transposition of the EU Fourth Money Laundering Directive into Irish law has also led to further enhanced international co-operation, as the Directive requires information to be shared between competent national authorities, including the creation of a central register of beneficial owners of entities.

© Law Business Research 2021

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

There is no generally applicable statutory obligation that creates an obligation on the police to keep information received during an investigation confidential.

Irish law does recognise a broad 'right to privacy', which is protected by the Irish Constitution, the EU Charter of Fundamental Rights and the European Convention on Human Rights. Further, data protection is regulated in Ireland primarily by the Data Protection Acts 1988–2018 (the DP Acts), which reflect EU data protection laws. The police are subject to the same obligation under the DP Acts as all data controllers, within the meaning of the DP Acts, when processing personal data. There are exceptions to the rules set out in the DP Acts, including where the processing is required to investigate or prevent an offence.

Whistleblowers are protected from identification by the Protected Disclosures Act 2014. Accordingly, great care must be taken not to violate these protections when an investigation involving whistleblower information is under way. However, the identity of whistleblowers can be disclosed to prevent a crime or to aid in the prosecution of a criminal offence.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In such circumstances, it would usually be prudent to advise the company not to provide the documents. However, the company should ensure that it is not violating any laws in its own jurisdiction by doing so. The company should inform the requesting authority of the basis for the decision to refuse the request for documents.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

The DP Acts regulate data protection in Ireland and protect the personal data of individuals from disclosure in certain circumstances. The transfer of data outside Ireland is restricted, but there is no outright 'block' preventing all transfers. The main implication of Irish data protection law is that companies may be reluctant to release materials in the absence of a legal obligation.

Further, care should be taken when releasing documents that relate to any type of contractual relationship, as there may be confidentiality terms in the contract or engagement terms that could be violated by the disclosure. A party should always be mindful that if it releases information without being compelled to do so, it is not protected from claims that it has breached Irish data protection legislation or breach of confidence claims.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

A company may be in breach of the DP Acts if it releases materials that contain personal data in the absence of lawful compulsion, and may also be in breach of confidence if it releases confidential material without being compelled to do so. There may also be other contractual consequences for a company releasing certain materials voluntarily. There is no automatic confidentiality attached to materials disclosed to law enforcement, unless restrictions have been agreed to that effect. Accordingly, material provided to authorities voluntarily may be shared with other authorities or used for purposes other than the initial basis of the request. Materials obtained on the basis of a compulsory power are subject to greater protections. However, once material is in the possession of an authority, there is nothing to prevent a third party from seeking the material, such as through a non-party discovery order.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Irish criminal legislation typically provides for monetary fines or terms of imprisonment for offences. Given the nature of corporate entities, the most common form of sanction is a fine. However, while less common, Irish legislation also provides for specific remedies, such as compensation orders and adverse publicity orders under health and safety legislation.

Common sanctions in the context of business crime are restriction and disqualification orders. Under section 839 of the Companies Act 2014, if a person has been convicted of an indictable offence in relation to a company, or convicted of an offence involving fraud or dishonesty, that person may not be appointed or act as an auditor, director or other officer, receiver, liquidator or examiner, or be concerned in any way, whether directly or indirectly, or take part in the promotion, formation or management of any company for a period of five years by default, but potentially longer should the court see fit.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Under the EU Public Sector Procurement Directive (2014/24/EU) (transposed into Irish law by the European Union (Award of Public Authority Contracts) Regulations 2016) companies must be excluded from public procurement for a specific period when they have been convicted of certain offences. The Regulations also provide for offences that carry discretionary debarment. These include offences under EU law, meaning that a company should take care when settling charges in another country, as doing so could, depending on the offence, trigger these exclusion rules.

The Regulations enable companies to recover eligibility to bid for public contracts by demonstrating evidence of 'self-cleaning', such as the payment of compensation to

© Law Business Research 2021

the victim, clarification of the facts and circumstances of the offence, co-operation with the investigating authority, and the implementation of appropriate measures to prevent further criminal offences or misconduct.

65 What do the authorities in your country take into account when fixing penalties?

Sentencing of corporate crimes is largely a function for the courts. If a business is found guilty of an offence, a wide range of factors may be taken into account at the discretion of the court. Mitigating factors include whether the company ceased committing the criminal offence on detection or whether there were further infringements or complaints; whether remedial efforts to repair the damage caused were used by the company; the existence of a compliance programme; and whether the company itself reported the infringement before it was detected by the prosecuting authority. Additionally, in imposing any sentence, the court must comply with the principle of proportionality as set out in *People (DPP) v. McCormack* [2000] 4 IR 356.

Certain sanctions, such as those available to the Central Bank of Ireland under the Administrative Sanction Procedure, or the Competition and Consumer Protection Commission in connection with cartels, can be expressed as a percentage of turnover.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No. There has been some consideration of these types of arrangements at policy level; for example, the Law Reform Commission recommended in its Report on Regulatory Powers and Corporate Offences (published on 23 October 2018) that deferred prosecution agreements (DPAs) be introduced, based on the UK model, which are subject to court approval. However, in December 2020, a report prepared by a review group chaired by former Director of Public Prosecutions James Hamilton, tasked with assessing the strategies and structures for investigation and penalising economic crime, refused to recommend DPAs in Irish law.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Neither non-prosecution agreements nor deferred prosecution agreements are available in Ireland.

© Law Business Research 2021

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

It is possible to enter into a settlement with some regulatory authorities in prescribed circumstances.

Generally, any company considering entering into a settlement with a regulatory or enforcement authority should balance the seriousness of the charge, the scope of a conviction, the strength of the case against it and against the terms of the settlement, such as the quantum of any fine, and whether there is publicity associated with the settlement.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The use of external corporate compliance monitors is not an enforcement tool used by Irish law enforcement authorities.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

A defendant may be subject to simultaneous civil and criminal proceedings arising out of the same set of circumstances. Although there is no obligation on the courts to do so, civil proceedings are commonly adjourned pending the outcome of related criminal proceedings. As there are different burdens of proof in civil and criminal matters, the outcome of civil and criminal proceedings will not necessarily be the same. It is also possible, although rare, for individuals to initiate private criminal prosecutions by issuing a summons pursuant to the Petty Sessions (Ireland) Act 1851 in certain limited circumstances.

Authorities are not obliged to disclose their files to such persons unless a particular file is generally open to the public or a court order has been obtained.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

The Irish judiciary is extremely protective of the accused's right to a fair trial and will prohibit or stay a trial if necessary. This sometimes occurs in respect of high-profile cases when the extent of publicity affects the ability of the defendant to have a fair jury trial. An example of this is the trial of a high-profile former chairman of Anglo Irish Bank, which was initially adjourned in 2015, owing to concerns of adverse publicity surrounding the trial.

Reports that undermine legal proceedings can amount to contempt of court. Further, any reporting that goes beyond a faithful account of the court proceedings could give rise to defamation claims.

Under new court rules introduced by the Data Protection Act 2018, an accredited member of the press may access documents that are 'opened' in court (i.e., read out in court by a lawyer or by the judge) and those that are 'deemed to have been opened' at a hearing before the court (i.e., documents that the judge has read in chambers and does not require the parties to formally open in court).

© Law Business Research 2021

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In larger companies, corporate communications are generally managed by a team of marketing professionals, and it is common for companies to employ public relations companies when there is a risk of negative publicity.

73 How is publicity managed when there are ongoing related proceedings?

It is important that any public statements issued by a company do not potentially prejudice ongoing criminal proceedings or investigations. Statements issued by a company in such circumstances should be brief, factual and approved by the company's legal advisers. Care should also be taken that no comments are made that potentially identify any persons, as there could be a risk of defamation proceedings if the statement incorrectly implies that a person has committed any wrongdoing.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Publicly listed companies on the Irish Stock Exchange must, without delay, provide to Euronext Dublin any information that it considers appropriate to protect investors. Euronext Dublin may, at any time, require an issuer to publish such information within the time limits as it considers appropriate to protect investors or to ensure the smooth operation of the market.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

The Disclosure of Non-Financial Information Regulations 2017 (SI 360/2017) transpose Directive 2014/95/EU (the Non-Financial Reporting Directive) into Irish law and requires directors of any company with more than 500 employees to:

- submit for each financial year a non-financial statement explaining the company's development, performance and position and the effects of its activity relating to environmental, social, human rights, and bribery and corruption matters; and
- include in its corporate governance statement a diversity report on the company's diversity policy and its implementation and results.

Regulation (EU) 2019/2088 (the Sustainable Finance Disclosure Regulation):

- requires financial market participants and financial advisers to disclose 15 different ESG considerations on their websites and in their remuneration policies and pre-contractual disclosures, including:
  - the principal adverse effects of investment decisions on sustainability issues;
  - the company's considerations of ESG and sustainability risks; and

© Law Business Research 2021

  - additional product-specific obligations where financial products promote environmental sustainability or have sustainable investment as their core objective; and
- introduces additional disclosure requirements for existing financial services legislation, including Directive 2011/61/EU on Alternative Investment Fund Managers, Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS), Directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II), Directive (EU) 2016/97 on insurance distribution and Directive 2014/65/EU on markets in financial instruments (MiFID II).

Regulation (EU) 2020/852 (the Taxonomy Regulation) requires financial market participants to disclose in pre-contractual disclosures and public reports:
- how certain financial products and their underlying investments in economic activities qualify as 'environmentally sustainable' under this Regulation; and
- in non-financial undertakings, the proportion of their turnover derived from environmentally sustainable products and services, and the proportion of their capital and operating expenditure relating to assets or processes associated with environmentally sustainable activities.

Regulation (EU) 2018/2089 (the Low Carbon Benchmark):
- requires benchmark administrators to include details of how they incorporate ESG factors in their benchmark methodologies and statements; and
- extends the period for national authorities to compel benchmark administrators to publish a critical benchmark from two years to five years.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Key legislative changes in coming years include a Corporate Sustainability Reporting Directive (which will revise the existing Non-Financial Reporting Directive, extend its obligations to companies with fewer than 500 employees and simplify the existing sustainability reporting process) and a regulation introducing a European green bond. Both proposals were still under European Parliament scrutiny as at August 2021.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

So far there has been limited ESG-related litigation in Ireland, but this may change following two developments. Ireland has until 25 December 2022 to implement Directive (EU) 2020/1828 (the Representative Actions Directive), which will introduce collective injunctive and redress measures for consumers for the first time. The Irish courts may also be receptive to ESG-related litigation following the Supreme Court decision in *Friends of the Irish Environment CLG v. The Government of Ireland & Ors* [2020] IESC 49, in which the Supreme Court quashed the Irish government's statutory plan for tackling climate change and held that climate change is already having a profound environmental and societal effect in Ireland.

© Law Business Research 2021

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

In September 2021, the government published the Companies (Corporate Enforcement Authority) Bill 2021, which will establish the Corporate Enforcement Authority (CEA), tasked with combating business crime and suspected breaches of company law. Under the Bill, the existing functions of the Office of the Director of Corporate Enforcement will transfer to the CEA, which will have a mandate to investigate a greater volume of cases and to target more complex types of offences.

The recently enacted Criminal Procedure Act 2021 introduces a number of significant changes to criminal procedure in Ireland, including the introduction of preliminary trial hearings, which should lead to efficiencies in the trial process. The Act awaits commencement.

In June 2021, the Minister for Justice published the General Scheme of the Garda Síochána (Powers) Bill. New measures included in the Bill include, inter alia, the introduction of a single power of arrest, putting the Garda caution on a statutory basis, and providing a power for the Gardai to require a person to provide passwords for access to electronic devices.

In April 2021, the government published an implementation plan of 22 actions to progress the 25 recommendations identified in the Hamilton Report.

There have been legislative changes to reflect the realities of the corporate environment during and following the covid-19 pandemic. The Civil Law and Criminal Law (Miscellaneous Provisions) Act 2020 and the Companies (Miscellaneous Provisions) (Covid-19) Act 2020 both came into effect in August 2020. The former Act seeks to address technical legal issues caused by the pandemic. Its provisions include the expansion of court powers to direct remote hearings, allowing for the electronic filing of court documents in civil proceedings, allowing business records to be used as evidence in civil proceedings, and widening the use of video technology in criminal proceedings.

© Law Business Research 2021

16

Italy

Enrico Di Fiorino and Lorena Morrone[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigations in Italy focus on international corruption involving the most important Italian companies, infiltration of organised crime in the economic sector and investigations against corporate giants for tax evasion. Italian criminal counsels observe the increased focus on regulatory topics, the higher number of dawn raids with a focus on companies' internal audit departments, the frequent use of precautionary measures and a growing involvement in cross-border investigations.

2 Outline the legal framework for corporate liability in your country.

Although the Italian system has always recognised a civil and administrative liability for companies, it did not provide for criminal liability in relation to companies until 2001.

This criminal liability is triggered if criminal offences included in a compulsory list have been committed by persons holding representative, administrative or managerial positions in a company, or by persons working under their control, provided that these persons have committed the crimes at least 'also' in the interests, or for the benefit, of the company, and the company cannot demonstrate that it has taken adequate measures to prevent the commission of the crimes.

Foreign companies can also be held criminally liable for crimes committed in Italy.

1 Enrico Di Fiorino and Lorena Morrone are partners at Fornari e Associati.

© Law Business Research 2021

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Several law enforcement authorities regulate corporations in Italy, including the Prosecution Service and independent administrative authorities.

Although the Prosecution Service has exclusive jurisdiction on investigations in relation to criminal matters, the independent administrative authorities, which have investigative powers and the power to impose sanctions, only have jurisdiction in specific matters, provided for by law.

As there are several enforcement authorities, the policies and protocols in this regard can differ. However, it is important to highlight that authorities usually have specific protocols relating to co-operation and the exchange of information.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Although the law does not provide for a threshold of suspicion necessary to trigger an investigation by certain independent administrative authorities, the public prosecutor shall immediately enter in the dedicated register any criminal data he or she receives or acquires, and then start a criminal investigation. The duty of the public prosecutor to bring criminal action is compulsory (not discretionary).

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Depending on the authority and type of notice, a company may challenge the lawfulness or scope of the notice or production order by way of an application to court.

As regards criminal proceedings, the lawfulness and the scope of a search warrant, and the production of documents or a seizure, may be challenged before the courts. However, subpoenas regarding summoning of witnesses are not challengeable. Witnesses have a duty to testify in front of a judge.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Italian law does not provide for a general application of immunity or leniency in recognition of co-operation with investigative authorities.

As regards criminal proceedings, Italian law has provided several case examples of leniency for specific offences, such as criminal organisation and drug trafficking, and – more recently – immunity (for example, with regard to fiscal-related offences in the case of a voluntary collaboration procedure, or crimes against the public administration).

© Law Business Research 2021

7 What are the top priorities for your country's law enforcement authorities?

The fight against national and international corruption has been a top priority for the Italian government and its law enforcement authorities for the past few years.

Tax evasion is also a key priority: in recent years, a set of new laws made the punishments for tax crimes harsher, introducing an enlarged model of confiscation and providing for vicarious corporate liability.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Compliance programmes in Italy are not mandatory but strongly recommended as they are necessary to avoid corporate criminal liability.

However, the adoption of a programme is not sufficient. Companies are required to prove that (1) the compliance programme has also been efficaciously implemented before the commission of the crime, (2) the person who committed the crime has fraudulently eluded it, and (3) the supervisory body has sufficiently monitored the company's activities.

Over the years, trade associations and professional orders (such as Confindustria) have issued numerous sets of guidelines to help corporations in implementing an effective compliance programme.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

During the past 20 years, a broad framework of laws has been developed (often as a result of international regulations). In particular, in 2018, Italy implemented the General Data Protection Regulation (GDPR) and Directive (EU) 2016/1148, concerning measures for a high common level in the security of network and information systems across Europe (the NIS Directive).

Moreover, Italy has ratified Directive (EU) 2018/843, which deals, among other matters, with the proper use of crypto-value to prevent money laundering.

Finally, Law No. 133/2019 provides for a series of obligations on public and private entities that carry out activities of public interest, to ensure the safety of information, systems and networks. Administrative sanctions shall apply in the event of non-compliance.

© Law Business Research 2021

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Italian law provides for a wide range of offences to prevent cybercrime. Over the years, law enforcement authorities (such as the Prosecution Service and the Italian Data Protection Authority) have given substantial attention to cybercrime.

The law punishes the conduct of hacking, phishing, infection of information technology systems with malware, possession of hacking tools, identity theft and electronic theft. Criminal offences have also been provided in the case of failure to comply with the security measures set out by the law and regulations issued by the Italian Data Protection Authority, unlawful data processing and any untrue or false statement sent to the Authority. Moreover, Law No. 133/2019 provides for a new crime in respect of false information or omissions that could impede or influence the effectiveness of the cybersecurity procedures established by the Law.

With regard to corporations, Italian law provides for financial penalties and disqualification in relation to cybercrime and illicit use of personal data.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Italian criminal law provides that the courts have jurisdiction on all offences committed within the Italian territory; that is, when at least part of the prohibited conduct takes place in Italy or the event of the crime occurs within the Italian territory.

Italy does not have general extraterritorial jurisdiction, although there are specific cases in which it will exercise extraterritorial jurisdiction (e.g., bribery involving Italian public officials and market abuse on financial instruments admitted on an Italian regulated market, even if the offences are committed abroad). Moreover, extraterritorial jurisdiction could be raised – under certain conditions – by means of the Italian nationality of the perpetrator or the victim, or even when a crime against the state is committed.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges derive from the need to identify which states have relevant jurisdiction and then the full co-operation of actions between the state in charge of the investigations and the other states, or all the competent agencies and organisations involved.

Co-operation is needed because of the existence of different laws and regulations in all the countries, mostly relating to privacy, professional privilege regimes and labour laws.

To facilitate coordination among (at least) the EU Member States regarding criminal matters and accelerate cross-border investigations, Directive 2014/41/EU regarding the European Investigation Order in criminal matters came into effect in July 2017. There are also bilateral and multilateral agreements between Italy and states that are not within the European Union.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Pursuant to the provisions of the conventions to which Italy is a party, the international principle of *ne bis in idem* can only be applied in the event of *res judicata* (final judgment). There is no prohibition against two criminal proceedings on the same cause of action against the same person or corporation taking place at the same time in two European countries.

It is worth highlighting that in *Mihalache v. Romania* (8 July 2019), a Grand Chamber of the European Court of Human Rights stated that the public prosecutor's order discontinuing criminal proceedings while imposing a fine on the applicant was a 'final acquittal or conviction'. This triggers the application of the *ne bis in idem* principle, based on a series of criteria which are in line with those relied on by the Court of Justice of the European Union in similar cases.

At the EU level, Council Framework Decision 2009/948/JHA provides for a mechanism of 'consultation' among the Member States with the aim of achieving a consensus on any 'agreed' solution so as to avoid parallel proceedings in different Member States.

At the international level, there is the principle of *lis alibi pendens*, but no specific rules aimed at settling the issue of proceedings that are pending simultaneously.

There are no measures in Italy that are comparable to the US 'anti-piling on' policy.

14 Are 'global' settlements common in your country? What are the practical considerations?

To date, there have been no global settlements involving Italy. However, Italian law does provide for a specific discipline regarding the execution of decisions of foreign states.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions of foreign authorities do not impede Italian investigations from going forward. Nevertheless, the law provides for final judgments issued by foreign authorities to be recognised in relation to specific aspects (such as reparation or recidivism). When there are international agreements for recognition in force between the parties, the Italian Code of Criminal Procedure provides for the possibility of enforcement in Italy, according to Italian law. Moreover, a 2010 law provides for a new type of mutual recognition of foreign criminal judgments, when they order a minimum of three years' detention.

© Law Business Research 2021

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Italy is required to observe and enforce UN Security Council sanctions and EU restrictive measures. Furthermore, the European Union applies restrictive measures for the purposes of pursuing the specific Common Foreign and Security Policy objectives or UN Security Council Resolutions.

The restrictive measures imposed by the European Union can target the governments of third countries as well as non-state entities or physical or legal individuals; for example, embargoes on the sale of weapons, other specific or general trade restrictions (import or export bans) or financial restrictions.

Member States are obliged to undertake specific tasks regarding implementation of the measures. The Financial Security Committee is the authorised agency in Italy in charge of monitoring the system for the prevention and sanctioning of money laundering and the financing of terrorism.

The aim of an Italian law issued in 2018 is to organise and simplify the authorisation procedures for the export of dual-use items and technologies.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

In recent years, the European Union has often made recourse to the imposition of sanctions or restrictive measures both autonomously and in compliance with the binding resolutions of the UN Security Council.

The Italian authorities do not show a strong interest in the execution of sanctions.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

At the European level, Member States co-operate with each other, for example, as regards authorisation for European operators who intend to work in Member States affected by trade embargoes.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The European Commission adopted Council Regulation (EC) No. 2271/96 against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (the EU Blocking Regulation), which is directly enforceable in Italy. The measure forbids EU citizens from complying with third-country extraterritorial sanctions unless exceptionally authorised to do so by the European Commission. In August 2018, the Regulation was expanded to curtail the effects of the United States' withdrawal from the Joint Comprehensive Plan of Action.

© Law Business Research 2021

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

The EU Blocking Regulation has not been subject to any binding judicial interpretation. Moreover, with the exception of the European Commission's non-binding Guidance Note – Questions and Answers: adoption of update of the Blocking Statute, no further official guidance has been adopted at a local level by Italian authorities.

Furthermore, no cases have yet been brought before the national courts.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

An allegation of misconduct could come to light through a report by a whistleblower, made according to a company's procedure. Furthermore, an internal investigation could follow the execution of investigative acts, carried out by the Prosecution Service or by an independent administrative authority. Finally, an investigation could be specifically requested by the supervisory body, if anomalies have come to light in the execution of its activity. Similarly, news spread by the media regarding alleged misconduct perpetrated by an executive or an employee could suggest an opportunity for a compliance check, carried out by internal or external auditors.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The main Italian legislation for the protection of personal data is the Privacy Code, amended according to the General Data Protection Regulation (GDPR). There are several sector-specific pieces of legislation that could affect a data protection regime, such as the Statute of Workers, the Consumer Code and the Telemarketing Law, and legislation on whistleblowing.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Data Protection Code provides for both administrative fines and criminal penalties.

The GDPR introduced an antitrust-type sanction regime with fines of up to 4 per cent of annual global turnover or €20 million, whichever is greater. A limited number of breaches fall into a lower tier and so are subject to fines of up to 2 per cent of annual global turnover or €10 million, whichever is greater. Regulators have a range of other powers and sanctions at their disposal.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

It is necessary to be aware of the potential conflicts between data privacy concerns and the need for gathering information that implies the processing of employees' personal data.

© Law Business Research 2021

Personal data shall be processed lawfully, fairly and in a transparent manner, and collected for specified, explicit and legitimate purposes. The affected employees shall be informed about the subject and purpose of the investigation, and their rights under the data protection laws. Additionally, in compliance with the principle of data minimisation, it shall be ensured that employees' personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

According to local employment law and the Italian Data Protection Authority, a company is prohibited from mass control and unlimited storage of employees' company emails.

Companies should adopt specific internal guidelines, for approval by trade unions and publicised internally, to enable the employer to carry out controls on employees' internet files and emails, with specific reference to making employees aware of the fact that the employer may execute controls on the data during internal investigations.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

If there are reasonable grounds to believe that the *corpus delicti* (the item on which, or through which, the offence has been committed or the profit made from the crime), or material items relating to the crime, are located on a company's premises, a search of those premises could be ordered by the public prosecutor.

At the beginning of the search, the accused and the person who has current access to the premises shall be given a copy of the decree ordering the search, with the notice informing them of their right to be assisted by a trusted person.

In the event of seizure ordered by the judicial authority, the person from whom the objects have been seized and the person who would be entitled to their restitution may submit a request for the re-examination of the seizure decree. The request does not suspend the enforcement of the decision.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The law provides for a duty to hand documents and documentary evidence to the requesting judicial authority, except if the person who possesses them by virtue of function, job, service or profession declares in writing that they are covered by either public service or professional secret. The judicial authority shall proceed with the necessary ascertainment if it has reasons to doubt the legitimacy of the declaration and if it cannot proceed without gathering the documents. If the declaration is groundless, the judicial authority shall order the seizure, which can be challenged with a request for the re-examination of the seizure decree.

© Law Business Research 2021

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

A witness is obliged to appear before the court, follow the judicial indications and answer truthfully the questions addressed.

If a witness fails to appear, without legal impediment, the court may order his or her compulsory appearance and that he or she pays a fine and the costs arising from the failure to appear. However, if the witness is a foreign citizen, Italy will not be able to enforce the aforementioned sanctions, given lack of jurisdiction. However, some mutual assistance treaties have been signed, which allow Italian enforcement authorities to ask for co-operation.

A witness is not obliged to testify on facts that could lead to self-incrimination. Moreover, the law provides for a right of abstention for the next of kin of the accused and for persons who invoke either public service or professional secret.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The protection scheme for whistleblowers is applicable only when the company has adopted an organisational model for crime prevention. In all cases, the whistleblower's identity is and must be kept strictly confidential.

There are no incentives provided for in relation to reporting individuals.

A whistleblower is protected from any retaliatory or discriminatory dismissal as a consequence of his or her reporting, and protection from a demotion or any other (direct or indirect) discriminatory or retaliatory measure as a consequence of the reporting.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

In relation to internal investigations, the Italian legislator sought to regulate the scope and the limits of companies' powers, to find a balance between the right of the corporation to protect its interests and assets and the protection of employees from any kind of abuse.

The Italian Workers' Statute and the General Data Protection Regulation require the observance of certain formalities in conducting the investigations (for example, the employee deemed to have engaged in misconduct has to receive a complete report about the ongoing investigations, with regard to the procedure, the scope and the corporate functions involved; in checking the corporate tools – such as laptops or lockers – the principles of necessity, relevance and no excess have to be respected) as well as in commencing a disciplinary proceedings against the employee who has been found guilty of the misconduct during the investigation.

There is no distinction for these purposes between officers and directors.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

All employees' rights are safeguarded in the context of internal investigations. A difference can be noted in the ways in which an employer can terminate an employment contract, depending on the type of misconduct: (1) dismissal without notice for just cause (e.g., where there is a serious breach of the employment contract, such as gross misconduct); or (2) ordinary dismissal with notice based on either a subjective reason or an objective reason. In either case, a special disciplinary procedure must be followed: the employer must promptly send the employee a letter describing the facts that would constitute a breach of the contract, wait for the employee's reply (which must be received within five days) and finally send the employee a letter of dismissal. If an employee is suspected of misconduct, but the company still needs to carry out an internal investigation to ascertain whether that suspicion is justified, precautionary suspension can be implemented until the end of the investigative procedure.

Suspension is not mandatory and does not deprive the employee of salary unless this is expressly provided for by the national collective contract of the particular sector or by the contract. Once the investigation is concluded, in a case of dismissal because of misconduct, the company could ask for the return of the undue salary that has been paid during the period of suspension.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

There is no obligation for employees to take part in an internal investigation. However, from a disciplinary standpoint relating to a general duty of co-operation with the employer or specific provisions in a company's policies, a refusal to participate may be relevant.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

A company is advised to begin each investigation with a carefully drafted action plan, which should identify the following:

- allegations of misconduct or concerns as reported by internal control bodies or whistleblowers, or resulting from media speculations or acts of an investigation;
- the functions and external parties who will manage and conduct the investigation;
- all the conceivable actions to be carried out (documentation to be analysed and individuals to be interviewed);
- the time frame for the investigation; and
- if an external counsel is appointed, how legal privilege will be maintained.

© Law Business Research 2021

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are generally no formal legal obligations on a company to conduct an internal investigation. However, conduct rules issued by regulators may mean an internal investigation is required under those rules, or at least strongly recommended.

When an issue comes to light, it is strongly recommended to take all necessary steps to stop the offending behaviour, if it is continuing, to protect and preserve all material that would be relevant and to adopt preventive measures to ensure that the behaviour cannot occur again.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

This decision depends on the individual circumstances of the case and the nature of the request.

Under the Italian Criminal Code, it is illegal to interfere with an investigation by a law enforcement authority (for example, by destroying evidence). In addition, corporations have statutory obligations to preserve documents for certain periods (in general for 10 years).

From a strategic point of view, a company should evaluate opportunities for co-operation. In many cases, it is advisable to co-operate so as to prevent coercive measures and reputational damage.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is generally no requirement for privately held corporations – with no reporting obligations under the securities laws – to publicly disclose the existence of an internal investigation or contact from law enforcement.

However, listed issuers shall publicly disclose information of a precise nature, which has not been made public, relating to one or more issuers and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments. Therefore, these companies must consider whether the disclosure of an internal investigation or contact from law enforcement would be considered material.

37 How are internal investigations viewed by local enforcement bodies in your country?

There is currently no specific discipline that regulates internal investigations, and it is recommended that companies pay attention to a number of legal issues, such as data protection and employment law-related concerns, as well as the protection of whistleblowers.

© Law Business Research 2021

Internal investigations could be approached by companies either as a reaction to an investigation started by the Prosecution Service to gather elements useful for the defence as part of criminal proceedings, or to co-operate with the enforcement authorities to discover misconduct.

Additional caution should be taken when a judicial investigation is likely, for example speaking to potential witnesses could result in subornation or be seen as an attempt to obstruct the investigation.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Considering that communications between a company and its in-house lawyers are not privileged, it is advisable that internal investigations are carried out by external defence counsel.

To protect the documentation relating to an internal investigation, it is recommended that it be held at the premises of the lawyer (which cannot be inspected or searched), labelling any related communications as 'Privileged and Confidential' and restricting the circulation of privileged documents.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Professional secrecy is usually invoked by the attorney, but in the primary interest of his or her client, who could be either a corporation or a person.

In the case of companies, privilege applies if the information was exchanged (1) for the purpose of legal assistance and (2) with an independent, external lawyer who is not bound to the client by any employment relationship and is a member of the bar.

If the lawyer is assisted by other professionals – such as technical consultants or authorised private detectives – the privilege is extended to them.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Although the attorney–client privilege applies in relation to external counsel, the professional activity of an in-house counsel is neither recognised nor regulated by any legal provision or statute. In-house counsel cannot be admitted to the bar (with some limited exceptions) and thus are deprived of all rights and privileges attached to independent lawyers who are members of the Italian Bar.

© Law Business Research 2021

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The law provides for the attorney–client privilege to avoid intrusions that could hinder the defence; therefore, this privilege should certainly extend to foreign lawyers, provided that they are admitted to their national bar and their title is recognised by the Italian system. However, to date, there is no precedent from an Italian court to confirm this reasoning with specific reference to lawyers (only with regard to foreign private investigators).

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There is also no general concept of waiving privilege under Italian law.

Public prosecutors consistently state that they cannot expect waiver of the attorney–client privilege and that waiver could not be considered a prerequisite to obtain credit for co-operation. Nevertheless, submitting privileged documents to authorities is regarded, in general, as a co-operative step.

It is mandatory to discuss any initiative with the client. Divulging a professional secret without justification (or using it for one's own profit of that of a third party), and thereby procuring damage, is an offence.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The Italian legal system does not provide for waiver of privilege (neither general nor limited). However, with reference to criminal proceedings, the jurisprudence has stated that the privilege between a client and an attorney may suffer limitation and restrictions if the lawyer is suspected or accused in criminal proceedings. Even if there is no actual waiver, in these cases all the information becomes available to third parties by means of the gathering of that information in the trial dossier.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There is no direct legal effect in Italy for the fact that privilege has been waived in another country. However, waiving privilege in one country by submitting documents to third parties can result in a loss of privilege, considering, for example, that documents disclosed to non-protected persons could be seized if they have lost privilege.

In addition, co-operation between enforcement agencies would be likely to render the privilege theoretical.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privilege does not exist in Italy. However, according to the law, all documents concerning the defence's strategy and all the correspondence between the defending counsel and the client are privileged and cannot be gathered in the trial dossier.

© Law Business Research 2021

Documents and correspondence in the possession of the attorney that also involve other lawyers and other accused, and which relate to the proceedings and the defence strategy of the client, have to be considered as privileged to protect the client's rights of defence.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Privilege could be invoked by an attorney even if the defence activity is carried out with the assistance of third parties. It is possible to include third parties who are, among others, trainee lawyers, secretaries, authorised private detectives and technical consultants.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Italian law allows witnesses to be interviewed during an internal investigation (usually by an external counsel).

An employee is requested to co-operate with the investigation team with regard to any aspects connected to his or her role and tasks, and more broadly to any information learned as part of the job. In the case of a former employee, an interview may be carried out only with the consent of the person.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

In most cases it is preferable for the interviewer to be a lawyer, who acts in accordance with all the formalities provided for by the defence investigations provisions of the Italian Code of Criminal Procedure. This ensures that all findings remain exclusively available to the defence counsel and the client.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

If an internal investigation is carried out with the prerogatives of preventive defence investigations, the external counsel has to give the interviewee all the warnings as provided for by the law (such as their right to silence or not to give any statement). Moreover, the lawyer shall inform the employee about his or her role and the purpose of the interview, and shall stop the gathering of information if the interviewee makes statements revealing indications of guilt.

The aforementioned rules apply to both employees and third parties.

The Italian Workers' Statute provides for specific rules to avoid any kind of abusive activity by the employer.

© Law Business Research 2021

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Italian law requires certain formalities to be followed. For example, the lawyers give the witnesses a warning, then they ask the questions and listen to the answers, all of which is included in a report, which has to be signed by all the persons attending the interview.

Documents could be shown to the interviewee if necessary or helpful.

Generally, it is not possible for an employee to be assisted by a lawyer during an internal interview, unless the employee is already the subject of a criminal investigation or disciplinary proceeding.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

According to Italian law, there is no obligation for a private entity to report crimes to the competent authorities (only public officials have the duty to report what they become aware of within their professional activities). Moreover, a lawyer is not under any obligation to disclose incriminating evidence against a client.

However, there are specific laws that provide for this kind of duty in relation to certain crimes and specific individuals (e.g., the law on anti-money laundering and illicit funding).

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The decision to disclose the findings of an investigation could be encouraged by the positive effect that co-operation with the authorities could have on a judge when quantifying the penalty. Moreover, it can contribute to avoiding the application or determining the reduction of pretrial disqualifying sanctions.

No negative consequences are provided for by law in respect of a lack of co-operation. A company under investigation – or at trial – assumes the same position as the defendant; therefore the privilege against self-incrimination (or right to silence) is granted. Nevertheless, the attitude shown by the company could lead to greater reputational risk.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The steps to be taken depend on the specific case at issue and the authority involved but, in any event, there is no obligation to self-report. Italian law does not provide for benefits deriving from the disclosure of information gathered through internal investigations, and does not contemplate any limitation to the investigation activity and to the possibility for the prosecutor to file a request for committal to trial.

© Law Business Research 2021

It is important to consider in each case whether self-reporting could help in the settlement with the public prosecutor and avoid the application of a disqualifying measure.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The response will depend on the type of notice received by a company and which authority has sent it. In the case of a request for document production from the public prosecutor, the company will respond through its external legal counsel, which can also arrange a formal appointment with the authority. Meetings with the public prosecutor can be scheduled but usually they are accompanied by the filing of a pleading.

In the case of a notice received by other enforcement authorities (e.g., a chamber of commerce), under Law No. 689/1991, the company may submit a defence case, within 30 days of notification, asking to be heard.

55 Are ongoing authority investigations subject to challenge before the courts?

It depends on the kind of investigation.

Generally, a criminal investigation itself cannot be challenged before the courts but individual measures taken as part of the process (e.g., seizure of documents) can, when unlawful.

Italian law provides for the possibility to challenge a request by the public prosecutor to continue with the investigations after an initial term of six months has expired.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

In general, it is a requirement to answer all requests received from the authorities. However, in criminal matters, there are now several instruments to strive for mutual co-operation and joint action teams, to prevent unnecessary duplication of effort, from both the private and the public sides.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If the material is under the control of a company (even by means of a parent company, therefore with a right to take possession, inspect or take copies of a subsidiary's documents), it is required to look for and produce all the requested material, even if located in another country.

© Law Business Research 2021

It could be that the data protection legislation in the other country does not permit the removal or transfer of the data from that jurisdiction: the requesting authority will seek help through mutual legal assistance with the foreign state.

A parent company could also raise a self-incrimination issue that impedes the delivery of data or documents.

Instead, if the document is not under the control of the company but the holder is known, the company can ask for it or indicate to the authorities the identity of the holder.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

There are several EU Directives and bilateral and multilateral agreements between Italy and countries that are not EU Member States to facilitate coordination between enforcement authorities.

Italian tax law enforcement authorities regularly exchange information based on conventions against double taxation signed with other states.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

During criminal proceedings, the investigations are protected by secrecy, so the public prosecutor and enforcement authorities will not have to disclose information to third parties. However, some investigations are conducted within a mutual assistance regime, in which authorities co-operate and exchange all the data acquired in the respective country.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The advice given will depend on the specific case: in fact, a comparison should be made between the benefits of co-operating with the authority in the company's country and the legal risk of violating a rule in the other country. To achieve this, the company should analyse the relevant rules, and request the legal opinion of a lawyer in that country. In cases of gross and evident violation, the best option would be to submit the opinion received to the public prosecutor and to encourage a mutual assistance request directly from one authority to the other.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

A request by an authority is usually a sufficient reason for the disclosure of data, according to the Italian Privacy Code.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production can be regarded in a positive light by a judge, as can effective co-operation with the authorities. However, it can generally not be challenged before the courts. In criminal law, even if the investigative dossier is supposed to be protected by secrecy, the company should be conscious that, once a document has been handed to the public prosecutor, it is possible that it will be given to third parties.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Individuals could face financial penalties and detention, as well as seizure and ancillary penalties (such as disqualification).

In respect of vicarious criminal liability, Italian law provides for four types of penalties: financial penalties, disqualifying measures, seizure and publication of the judgment.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Legislative Decree No. 50/2016, which adopted Directive 2014/24/EU on public procurement, prohibits companies found guilty (in the previous five years) of specific offences (e.g., corruption, fraud, money laundering and terrorism) from competing for government contracts throughout the European Union.

65 What do the authorities in your country take into account when fixing penalties?

According to the Italian Constitution, penalties cannot consist of any treatment that is inhumane and must have the aim of rehabilitation of the convicted individual.

With regard to individuals, the judge takes into account the seriousness of the crime deriving from several aspects (such as the nature of the offence, the seriousness of the consequent damage, existing precedents, the subsequent conduct of the accused, and so on).

Corporations are punished with financial penalties based on a quota system, considering various factors: the seriousness of the deed, the degree of liability of the entity and the activity carried out by the entity to eliminate or diminish the consequences of the unlawful act and to prevent the commission of further unlawful acts. The judge also considers the economic and financial status of the entity.

© Law Business Research 2021

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Italian case law states that the law on probation is applicable only to individuals. Neither non-prosecution agreements nor deferred prosecution agreements are provided for.

It is possible for a corporation to settle a case in advance by means of a special proceeding known as an application of punishment upon request. The company may agree with the public prosecutor to request the court to impose a penalty (reduced by a maximum of a third), when:

- the employee, whose conduct triggers the corporate liability, settled the case by means of an application of punishment; or
- the only sanction applicable to the corporation is a financial one.

However, the agreement between the company and the public prosecution authority will be rejected by the judge if he or she feels a permanent disqualifying sanction is warranted.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Neither non-prosecution agreements nor deferred prosecution agreements are provided for by Italian law.

However, proceedings for vicarious liability against a corporate entity are automatically merged with proceedings for an underlying crime allegedly committed by an individual. Therefore, the judicial authority will be aware of the choice of the company in the case of, for example, an application of punishment upon request.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

A company should assess the strength of the prosecution and defence cases.

Adverse effects, such as damage to reputation, should be considered. According to Italian law, a settlement cannot be considered a confession of liability. However, an application of punishment shall be considered equal to a judgment of conviction, unless otherwise provided by the law.

International implications should also be considered, such as the effect in regard to ongoing investigations in other jurisdictions.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

External corporate compliance monitors are not used as an enforcement tool. In specific cases, the law provides for the appointment of a special commissioner (e.g., when a disqualifying measure should be applied, which results in the interruption of all corporate activities).

© Law Business Research 2021

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel civil actions are allowed. A civil action brought before the civil court may be transferred to criminal proceedings if, in the civil court, a judgment on merits has not been issued. If the action is brought against the accused in a civil court after joining the criminal proceedings as a civil party, or after a judgment of first instance is issued, civil proceedings shall be suspended until the delivery of a final criminal judgment. The plaintiff may have access to the public prosecutor's dossier.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under Italian law, investigative acts carried out by a public prosecutor and the police are protected by secrecy until the accused is entitled to have knowledge of them and, in any case, not beyond the closing of preliminary investigations.

Publication in the press of the aforementioned documents or their content, even if partially, is not allowed.

The publication, in whole or in part, of documents that are no longer protected by secrecy is not allowed until preliminary investigations are concluded or the preliminary hearing is terminated. However, if the proceedings reach the trial stage, publication (in whole or in part) of the documents in the investigative dossier is not allowed prior to the delivery of the appeal judgment.

Nevertheless, publication of the content of documents that are no longer protected by secrecy is allowed.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Corporate communication is a delicate aspect of management, which should always be evaluated carefully by experts and approved by the legal office and external legal consultants. An incorrect press release by a company could have a detrimental effect on customers and on the strategy eventually chosen during a trial.

The biggest companies in Italy rely on both internal and external professionals for public relations.

73 How is publicity managed when there are ongoing related proceedings?

It is a general rule that the court should not be influenced by press reports surrounding a trial. Therefore, during criminal proceedings, a company should avoid public communications and, when unavoidable, should make only brief and factual statements that have been approved by its external legal consultants.

© Law Business Research 2021

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Privately owned corporations with no reporting obligations under the securities laws are generally not required to publicly disclose the existence of a settlement.

However, listed issuers shall publicly disclose information of a precise nature, relating to one or more instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments. Therefore, these companies must consider whether the disclosure of a settlement would be considered material.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

The Italian legal framework includes numerous rules concerning ESG, including:

- Legislative Decree 152/2006 on environmental liability;
- Legislative Decree 231/2001 and Law 221/2015 on the green economy;
- Law Decree 111/2019 on air quality;
- Law 68/1999 (as modified by Legislative Decree 185/2016) on the rights of disabled workers;
- Legislative Decree 81/2008 on the protection of workers' health and safety in the workplace;
- Law 190/2021 on the adoption of anti-corruption models by companies owned or controlled by the state; and
- Regulation (EU) 2019/2088 on sustainability-related disclosures in the financial services sector on sustainable investment.

Law 208/2015 provides for 'benefit corporations', namely those that include benefits both for society and the environment in their mission, to be subject to ESG mandatory disclosures and to enjoy beneficial fiscal treatment.

With regard to ESG disclosure, Italy has enacted Legislative Decree 49/2019 (implementing EU Shareholder Rights Directives I and II), Legislative Decree 147/2018 (implementing Directive (EU) 2016/2341 on the activities and supervision of institutions for occupational retirement provision (IORPs) – European Pensions Directive IORP II) and Legislative Decree 254/2016 (implementing Decision 2014/95/EU on the mobilisation of the EU Solidarity Fund), which requires public interest entities to disclose sustainability into the reporting cycle and provides for a voluntary regime applicable to non-obliged companies.

The Italian National Action Plan on Business and Human Rights for 2016–2021 commits to implementing the United Nations' 17 Sustainable Development Goals.

© Law Business Research 2021

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Legal and regulatory developments are certainly expected and some are already on the horizon. Law 53/2021 mandates the Italian government to implement a set of European directives, including Directive (EU) 2018/2001 on renewable sources, Directive (EU) 2019/883 on port reception facilities for the delivery of waste, Directive (EU) 2019/904 on the reduction of the impact of plastic products, Directive (EU) 2019/944 on common rules for the internal market for electricity, Directive (EU) 2019/1152 on transparent and predictable working conditions in the European Union, and Directive (EU) 2019/1161 on the promotion of clean and energy-efficient road transport vehicles.

In 2019 and 2020, the National Commission for Companies and the Stock Exchange (CONSOB) and the Bank of Italy launched market consultations on proposed changes to their existing regulations regarding transparency of remunerations, asset managers and shareholders' activism as well as shareholders' identification, transmission of information and exercise of rights of listed companies' shareholders. Finally, national legislation is expected to be enacted in the coming years to implement Regulation (EU) 2020/852 on the establishment of a framework to facilitate sustainable investment.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

The first Italian greenwashing case was in January 2020, when an Italian oil and gas company was fined €5 million by the Italian Competition Authority for having launched a misleading marketing campaign for its Diesel+ fuel.

With regard to sustainability reporting, on 1 September 2020, CONSOB launched a call for evidence to collect information about the failure of the voluntary non-financial statements publication regime, suggesting useful updates to the national framework.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

There is an ongoing debate in Italy in relation to the possibility of making the implementation of compliance programmes mandatory, when requested to exclude corporate vicarious liability. Several law proposals aim to extend the crimes that could trigger vicarious liability.

There are increasing requests for the introduction of restorative justice to stimulate self-reporting by companies, in exchange for the possibility to reach a settlement with the enforcement authorities for the dismissal of a criminal case.

At the European level, considering that existing EU bodies lack the necessary powers to carry out criminal investigations for crimes against the EU budget, trust is placed in the European Public Prosecutor's Office, which started activity on 1 June 2021.

© Law Business Research 2021

17

New Zealand

William Fotherby, Britt Rorrison and Caitlin Anyon-Peters[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

CBL Insurance Limited (in liquidation) (CBLI) was put into liquidation on the application of the Reserve Bank of New Zealand (which is responsible for regulating the insurance sector) in November 2018. It applied to appoint liquidators following repeat failures by CBLI to meet solvency, direction and reporting conditions. The Reserve Bank subsequently commissioned a review of its own actions in overseeing CBLI to identify lessons for New Zealand's insurance regulatory regime.

CBLI's related entity, CBL Corporation Limited (in liquidation) (CBLC), was liquidated in May 2019. Following the liquidation of CBLI and CBLC, independent investigations were launched by New Zealand's Financial Markets Authority (FMA) and Serious Fraud Office (SFO) into the conduct of the companies and their directors.

In December 2019, the FMA filed two sets of civil proceedings against CBLC, its six former directors and its former chief financial officer alleging breaches of New Zealand's Financial Markets Conduct Act 2013. These proceedings are before the High Court of New Zealand.

Also in December 2019, the SFO filed criminal charges against some of CBLI's former directors and chief financial officer alleging theft by a person in a special relationship, obtaining by deception and false accounting. An eight-week trial of these charges was scheduled to commence in the High Court at Auckland in September 2021 but was adjourned for reasons relating to covid-19 restrictions.

1 William Fotherby is a principal, Britt Rorrison is a senior solicitor and Caitlin Anyon-Peters is a solicitor at Meredith Connell.

© Law Business Research 2021

Additional sets of proceedings have been commenced against the companies by their liquidators and shareholders.

2 Outline the legal framework for corporate liability in your country.

New Zealand's legal framework generally enables corporate liability for wrongdoing. Key statutes from a corporate liability perspective, including New Zealand's Interpretation Act 1999 and Crimes Act 1961, broadly define 'person' to include companies and other bodies, incorporated or not. Applying this definition, corporations may be held directly or vicariously liable for the conduct of their employees or agents.

Regulatory agencies routinely prosecute corporations for unlawful conduct resulting in ill-gotten gains. Examples include prosecutions brought by the Commerce Commission seeking fines against companies who have profited from unfair trade practices, or prosecutions brought by the Chief Executive of Land Information New Zealand against overseas investors that have unduly profited by circumventing New Zealand's overseas investment rules.

Although the general position is that corporations can be held liable for true crime, in practice, such prosecutions are rare. More commonly, true crime prosecutions (including financial crime) are instituted against a company's directors. Further, some offences cannot be interpreted as giving rise to corporate liability. Homicide, for example, is expressly defined as the killing of one human being by another.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

New Zealand has no central decision-making agency responsible for prosecution decisions. Crime is prosecuted by the New Zealand Police, Crown solicitors and a number of specialist government agencies responsible for enforcement within a particular regulatory area. Corporate regulation is frequently the responsibility of these specialist agencies, the creation and jurisdiction of which is statutorily mandated. Jurisdiction is generally discrete, but where there is overlap, agencies work co-operatively.

Key agencies (and their responsibilities) include the following:

- Commerce Commission (regulation of competition and consumer protection);
- FMA (regulation of financial services and securities markets);
- Inland Revenue Department (enforcement of tax law);
- Takeovers Panel (enforcement of compliance with New Zealand's Takeovers Code);
- Reserve Bank (regulation of banks, insurers and other deposit-takers);
- SFO (prosecution of serious or complex financial crime); and
- WorkSafe (regulation of workplace health and safety).

To unify these various bodies responsible for making prosecution decisions within New Zealand, the Solicitor-General promulgates Guidelines for Prosecutions that set standards to guide prosecution decisions. In addition, the various agencies frequently publish their own policies and procedures.

© Law Business Research 2021

A broader range of government departments have a role in investigating and enforcing corporate regulation outside of the criminal jurisdiction. For example, the Ministry of Education is responsible for the regulation of corporates providing education services.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Enforcement agencies within New Zealand are independent. They exercise a high level of discretion in making investigation and prosecution decisions within their regulatory area.

Agencies generally publish investigation and enforcement guidelines outlining the factors relevant to their decisions. Their ability to escalate a complaint is further constrained by any statutory limits on their use of powers, and by practical limits. Of course, agencies must also uphold the rights of individuals (for example, the right to be free from unreasonable search and seizure or unlawful detention), which are enshrined in New Zealand's Bill of Rights Act 1990.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The actions of enforcement agents, including the issue of notices or subpoenas, can be challenged in New Zealand by way of judicial review. The challenging party applies to the High Court seeking review of the impugned decision. The grounds on which a review can be brought are limited: the challenging party must identify a defect in the decision-making process or demonstrate that the decision was otherwise unreasonable. The outcome of a successful review will be that the court refers the matter back to the original decision maker for a new decision. An example of such a challenge to an SFO warrant can be found in *A Firm of Solicitors v. District Court at Auckland* ([2006] 1 NZLR 586 (CA)).

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Co-operation with authorities is a mitigating factor relevant to enforcement outcomes or sentencing. Enforcement guidelines provide specifically for the consideration of co-operative behaviour within each regulatory field. Defendants are frequently granted a discount on sentence in recognition of their co-operation with an investigation, for example, for making voluntary disclosures, attending voluntary interviews or providing documents. Defendants may also be granted a discount on sentence if they have provided assistance with broader investigations against others.

The Solicitor-General's Prosecution Guidelines provide that the Crown may grant a witness immunity from prosecution. Immunity is granted by way of a written undertaking from the Solicitor-General that any subsequently initiated prosecution will be stayed. Immunity will only be considered in respect of very serious offending and when the witness has relevant evidence that significantly strengthens the Crown's case and was a minor participant in the offending only.

© Law Business Research 2021

7 What are the top priorities for your country's law enforcement authorities?

Each discrete regulatory area sets its own priorities and direction, though these generally bear synergies. Key shared priorities for New Zealand's law enforcement agencies at present are the prevention of organised crime, bribery and corruption and the management of New Zealand's covid-19 response.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

New Zealand companies are not required to implement formal compliance programmes. Online guidance is available to assist corporations to comply with their key financial, company law and employment obligations, including through the New Zealand Companies Office website. Companies may outsource aspects of their compliance obligations to certified compliance organisations – affiliation with such an organisation is deemed proof of compliance with a particular aspect of the law. This arrangement is common with consumer goods and services, such as the compliance of certain building products with the technical requirements of the New Zealand Building Code. It is generally recognised that reliance on a compliance organisation reduces a corporation's culpability if it is later found not to comply with an obligation for which it was certified.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Cybersecurity is a developing area of regulation in New Zealand in recognition of the growing threat posed by cybersecurity attacks. At present, New Zealand does not specifically regulate cybersecurity and corporations are not held liable for merely having weak or lax cybersecurity protection. However, corporations may become liable for the consequences of weak or lax cybersecurity where those consequences are regulated, for example, through New Zealand's privacy and data protection regime.

A recent example follows the ransomware attack of a regional district health board (DHB) in May 2021, which saw the distribution and publication of patient information. Following that incident, New Zealand's Privacy Commissioner confirmed that the DHB would not be fined for its patient data being hacked, but it may face liability if it is found that harm was suffered as a result. Enforcement powers are being strengthened in this regard. The Privacy Commissioner gained new powers to issue compliance notices under the Privacy Act 2020, and has indicated that these powers could be used to require entities to fix identified vulnerabilities in their security.

Cybersecurity is generally a governance matter for individual organisations. However, the National Cyber Security Centre provides assistance to the most significant

© Law Business Research 2021

public and private organisations to protect their information systems from advanced cyber-borne threats.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

New Zealand routinely prosecutes cybercrime at a domestic level. The Crimes Act 1961 criminalises an increasing range of cyber offences, including in relation to the unlawful access and use of computer systems, scams and harmful digital communications. Cyber offences attract a range of penalties. The maximum penalty for a cybercrime is 10 years' imprisonment for a person who intentionally or recklessly destroys, damages or alters a computer system knowing (or where they ought to have known) that danger to life is likely to result (Crimes Act 1961, section 250).

New Zealand's Cyber Security Strategy 2019 recognises the importance of international partnerships to combat transnational cybersecurity threats. It supports a free, open, secure internet and the development of a rules-based order to promote peace and stability online. New Zealand recognises that international law applies online as it does offline, including the United Nations Charter, the law of state responsibility, international humanitarian law and international human rights law. In February 2021, the government announced that New Zealand will join the Council of Europe Convention on Cybercrime (the Budapest Convention) following the recommendation of the Royal Commission of Inquiry into the Christchurch terror attack and consultation with the New Zealand public. Amendments to New Zealand's domestic legislation are required prior to formal accession.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, criminal law in New Zealand does not have extraterritorial effect (see Crimes Act 1961, section 6). However some specific offences are criminalised extraterritorially, including participation in organised crime, bribery and corruption, and money laundering.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations and litigation require reconciliation of different legal and cultural environments. Challenges are greatest when the jurisdictions involved do have significant legal and cultural differences. In our experience, the following challenges commonly arise in cross-border investigations and litigation:

- dealing with different offices in different countries and differences in how they store their own data that an investigation may require;
- ensuring regulatory requirements in each country comply with the law of the country in which an investigation or proceeding is initiated;

© Law Business Research 2021

- facilitating data transfer between jurisdictions and ensuring compliance with legal requirements in the home jurisdiction (in the case of New Zealand, most relevant is the Privacy Act 2020);
- coordinating with lawyers in other jurisdictions, especially where there are significant time-zone differences;
- anticipating and overcoming language and cultural barriers to ensure full and consistent understanding of all interested parties; and
- obtaining reliable translations of important documents.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The law in New Zealand protects against double jeopardy within the New Zealand context. The Crimes Act 1961 provides that no one (including a corporation) is liable to be punished twice in relation to the same offence (section 10(4)). This is further mirrored in the New Zealand Bill of Rights Act 1990 (note that this is an ordinary statute, not a constitutional document of higher order) in which section 26(2) provides that a person cannot be tried or punished for an offence for which they have been finally acquitted, convicted or pardoned. However, a person or corporation can be charged with two separate offences arising from the same act or omission, provided the elements of each offence have discernible differences.

New Zealand does not have any equivalent to the 'anti-piling on' policy of the United States.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common, probably because multinational corporations do not tend to have a base in New Zealand.

However, New Zealand can request from and provide assistance to other countries in relation to criminal matters: this framework for co-operation is contained in the Mutual Assistance in Criminal Matters Act 1992.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

The decisions of foreign authorities are given weight in New Zealand, but will not preclude New Zealand authorities and institutions conducting their own assessment or investigation.

An example is the New Zealand Supreme Court's judgment in *Minister of Justice v. Kim* ([2021] NZSC 57). China requested that Mr Kim be extradited to China to face a charge of murder. The request assured that, if convicted, Mr Kim would not face the death

© Law Business Research 2021

penalty. The New Zealand Minister of Justice decided that Mr Kim should be surrendered for extradition, but Mr Kim successfully reviewed that decision up through the courts. In reviewing the Minister's decision to extradite, the Supreme Court closely considered the human rights situation in China, including the risks of an unfair trial and torture.

The *Kim* judgment indicates that requests and assurances from overseas authorities will not be taken at face value, and that New Zealand will carefully consider its international obligations.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

New Zealand is a Member State of the United Nations and, as such, is bound by the decisions of the United Nations Security Council. New Zealand individuals and companies must comply with locally enacted regulations relating to UN sanctions.

Breach of UN sanctions regulations is a criminal offence. The following maximum penalties can be imposed for such offending:

- by an individual, imprisonment for a term not exceeding 12 months or a fine not exceeding NZ$10,000; or
- by a company or other corporation, a fine not exceeding NZ$100,000 per offence.

The first prosecution in New Zealand for breach of UN sanctions was of an aircraft company that had breached the sanctions by exporting aircraft parts to North Korea. It was fined just under NZ$75,000 (*New Zealand Customs Service v. Pacific Aerospace* [2018] NZDC 5034). This fine followed a guilty plea to three charges and the judge's finding that the company's conduct was reckless rather than intentional. Had the judge found that the company possessed knowledge or intent to breach sanctions, the fine is likely to have been higher.

New Zealand does not have legislation in place to impose its own autonomous sanctions. However, a Bill is currently going through Parliament that seeks to establish such legislation. Previous Bills of a similar nature have not succeeded.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

As a UN Member State, New Zealand implements UN Security Council sanctions through domestic regulations made under its United Nations Act 1946. But New Zealand does not have an autonomous regime and cannot impose unilateral trade and financial sanctions. This limits the country's ability to take meaningful enforcement action against UN veto holders and their close political allies. In recent years, New Zealand has explored the possibility of implementing an autonomous sanctions regime. In this context, an amended Autonomous Sanctions Bill is presently before Parliament following the failure of a predecessor Bill in late 2020.

© Law Business Research 2021

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

New Zealand authorities actively co-operate with foreign authorities in relation to criminal matters, and there is no reason to think this not the case in the area of sanctions compliance and enforcement.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

No.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not relevant.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Most allegations of misconduct come to light through the activities of whistleblowers. Whistleblowing is currently governed by the Protected Disclosures Act 2000. A replacement Bill is before Parliament, which seeks to expand whistleblower protections somewhat, particularly around risks of retaliation. It is not clear when Parliament will enact this Bill and in what form. However, like other areas dealt with in this chapter, whistleblowing is an area in which employee rights form an important background to initial steps taken in any investigation.

Prospective purchasers do not always conduct white-collar due diligence in the course of mergers and acquisitions, which makes this type of due diligence a less likely identifier of misconduct. Similarly, New Zealand's use of suspicious activity reports is less intensive than in other jurisdictions, although the practice is steadily increasing (reports are filed monthly on the New Zealand Police website).

Internal and external auditors do not have a significant history of identifying misconduct in New Zealand. That said, one of the highest-profile recent corporate investigations is into alleged inappropriate accounting at Fuji Xerox's New Zealand subsidiaries. The investigation commenced following the company's change of audit firm, and the issuing by the new auditors of a letter identifying potential fraud. Another event in the lead up to this investigation was a series of reporting by a New Zealand business publication following the public filing of financial statements with the New Zealand Companies Office.

Finally, one more common (if belated) route to unearthing corporate misconduct is the appointment of liquidators or interim liquidators by company creditors or regulators. The liquidators will then conduct an investigation into the company's affairs. The investigations into CBL Insurance Limited (in liquidation) began following the appointment

© Law Business Research 2021

of interim liquidators to the company, on the application of the Reserve Bank, following significant overseas payments in breach of directions by the regulator.

INFORMATION GATHERING

22 Does your country have a data protection regime?

New Zealand's data protection regime is governed by the new Privacy Act 2020. Among other things, the new Act gives the Privacy Commissioner greater powers to issue codes and practice, compliance notices, and to prohibit the cross-border transfers of personal information.

While the Act makes reference to guidelines of the Organisation for Economic Co-operation and Development (OECD) and to the EU General Data Protection Regulation (GDPR), it does not provide the same range of rights for data subjects as this latter directive. For example, there is no right to be forgotten. The Act does expand the Privacy Commissioner's enforcement power, but this power is limited to the issuing of compliance notices with a penalty for non-compliance of up to NZ$10,000. As part of the Act's drafting process, the New Zealand Law Commission considered the ability to impose larger fines, as is available in European jurisdictions, yet the Commission chose to begin with the compliance notice power (as now enacted) and assess whether the power would need to be augmented to increase the Act's effectiveness.

One of the major introductions in the Act is a new information privacy principle that deals with cross-border data transfers. An organisation covered by the Act may only send personal information outside New Zealand in a limited number of situations, as set out in the Act. The Privacy Commissioner also can prohibit cross-border transfers where the recipient country does not have legal safeguards comparable to those in the Act and the transfer would be likely to contravene basic principles set out in the OECD guidelines (for instance, although New Zealand currently has an adequacy decision from the European Commission, the Commission intends to reassess this decision in light of the GDPR). The Privacy Act also introduces compulsory notification requirements in the case of certain types of data breach.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Privacy Commissioner enforces the Privacy Act 2020. Although the new Act appears to signal a more interventionist role for the Commissioner, how it will exercise its new powers in practice remains to be seen.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Cross-border transfers of personal information need special care in the course of an internal investigation under New Zealand law, and this issue is likely to attract greater attention under the Privacy Act 2020 than it did under its predecessor.

© Law Business Research 2021

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Usually, an employee's employment agreement will specify the rights an employer has to intercept employees' communications. It is common for the employment agreement, or the employer's policies, to allow employers to monitor or review employee work communications in specified circumstances.

If the communications are not on work devices, or use work emails, then the provisions of the Privacy Act 2020 will determine the extent to which employers can collect this information. Information Privacy Principle One, for example, prohibits an organisation collecting personal information other than for a lawful purpose or if collection is necessary for a function of that organisation.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Raids by the Serious Fraud Office (SFO) are not uncommon. The director of the SFO has the power, under the Serious Fraud Act 1990, to apply for a search warrant if there are reasonable grounds for believing that information provided through a compulsory section 9 interview is false or misleading in a material way, that a person has failed to comply with his or her section 9 obligations, that it is not practicable to serve a notice under section 9, if a person cannot be located, is missing or there is any other good cause, or where the service of a section 9 obligation might seriously prejudice the investigation. The court must also be satisfied that there are reasonable grounds for believing that relevant documents may be found at the specified location.

By contrast, the New Zealand Police's Financial Crime Group uses traditional police investigation techniques, reliant on surveillance, the execution of search warrants and evidential interviews under caution.

Where a prosecuting agency may have exceeded its powers, the subject of these powers may challenge their exercise by judicial review, or, if charges are laid, by seeking to exclude evidence obtained by these powers under section 30 of the Evidence Act 2006.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Section 102 of the Search and Surveillance Act 2012 prevents a search warrant being issued for any communication covered by legal professional privilege. The exception to this bar is when an issuing officer is satisfied that there is a prima facie case that the communication or other thing sought was produced either for a dishonest purpose or for the purpose of planning to commit an offence.

© Law Business Research 2021

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Section 27 of the Serious Fraud Office Act 1990 removes the common law privilege against self-incrimination where a person is interviewed under section 9 of the Act. These powers are similar to those enjoyed by the UK's Serious Fraud Office. However, a self-incriminating statement will only be admissible in a subsequent prosecution if a person gives evidence inconsistent with the earlier incriminating statement.

Where not explicitly excluded in this way, New Zealand law otherwise recognises a robust right against self-incrimination.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Protected Disclosure Act 2000 (the Act) currently governs whistleblowing in New Zealand. A replacement Bill is currently before Parliament, but it is unclear when it will become law.

Both the existing Act and the replacement Bill set out the legislative goal of promoting the disclosure and investigation of matters of serious wrongdoing, and the protection of employees who make disclosures. But, at present, the protections for whistleblowing largely only exist in relation to wrongdoing in the public sector. One of the key changes the Bill proposes is to widen coverage to the private sector as well.

Under the current regime and its proposed replacement, the focus is on protecting whistleblowers from retaliation. The Act provides several legal protections. These protections include protection from retaliatory action, confidentiality of identity, immunity from civil, criminal and disciplinary proceedings and remedies for victimisation under the Human Rights Act 1993 (sections 18 and 19). Note that, like the equivalent UK legislation, the protection is one for employees to raise themselves, usually in the context of proceedings relating to their employment. The new Bill makes clear that an employee who faces retaliation will have a personal grievance against his or her employer under New Zealand's Employment Relations Act 2000.

Under both regimes, although the recipient of a protected disclosure must use 'best endeavours' to keep the identity of a whistleblower confidential, there are a number of exceptions to this principle. These exceptions include where the person who has acquired knowledge of the protected disclosure reasonably believes that disclosing the information is essential:

- to the effective investigation of the allegations in the protected disclosure;
- to prevent serious risk to public health or safety; or
- having regard to the principles of natural justice.

There is no financial incentive scheme in New Zealand for whistleblowers.

© Law Business Research 2021

Although whistleblower policies are only mandatory for public sector agencies (Protected Disclosures Act 2000, section 11(1)), the Bill proposes giving the New Zealand Ombudsman (the public sector regulator) power to ask private organisations for details of their whistleblowing procedures and practices for the purposes of administering the law.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There is a significant employment aspect to all investigations. Many issues that arise in the course of an investigation into potential wrongdoing within an organisation will be framed as employment issues first, and issues of corporate liability second. Moreover, some of the highest-profile corporate investigations have examined issues relating to workplace culture and conditions (examples include recent investigations into allegations of sexual harassment at the law firm Russell McVeagh, and the media company Mediaworks).

Employee rights in the course of an investigation are governed by the test of justification in section 103A of the Employment Relations Act 2000. This test assesses whether any employer action was what a fair and reasonable employer could have done in all the circumstances at the time the action occurred. The test is objective.

In the event that an investigation leads to the dismissal of an employee, or some other adverse action, in assessing reasonableness, the specialist employment tribunals will look to the resources available to the employer and whether the employer sufficiently investigated the allegations against the employee. It will also be relevant whether the employer raised its concerns fairly with the employee and gave him or her a reasonable opportunity to respond (Employment Relations Act 2000, section 103A(3)). So, an employee whose conduct may be impugned as a result of an investigation has significant protective procedural rights: essentially a right to a fair process, which is central to New Zealand employment law.

Company directors who are also employees have the same rights as non-director employees.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Principles of natural justice apply to employees suspected of misconduct. Although an employer has the right to take disciplinary action if it believes an employee has engaged in misconduct, and this misconduct justifies a particular disciplinary action, the employer is required to treat all cases of suspected misconduct fairly.

A fair process involves the employer advising an employee of the details of the allegations, providing a reasonable opportunity to respond, and considering any explanations fully before concluding that disciplinary action is required.

Usually, this process will involve suspending the affected employee (if the employment agreement allows it or the employee agrees) if the employer cannot carry out a proper investigation with the employee still in the workplace.

© Law Business Research 2021

New Zealand's Employment Court has commented that even an employee involved in a criminal proceeding might not inevitably be dismissed. The question remains whether the employee's conduct meets the criteria for dismissal in the relevant employment agreement (*Hallwright v. Forsyth Barr Ltd* [2013] NZEmpC 202 at [83]).

32 Can an employee be dismissed for refusing to participate in an internal investigation?

It is unlikely that, by itself, a refusal to participate in an internal investigation would justify an employee's dismissal, unless there were circumstances that made the act of refusal 'destructive of that basic confidence or trust that is an essential of the employment relationship' (*Northern Distribution Union v. BP Oil New Zealand Ltd* [1992] 3 ERNZ 483 (CA) at 487).

However, when the scope of an investigation includes whether an employee has been guilty of underlying misconduct, and the employee chooses not to participate having been given a fair opportunity to do so, then an employer can fairly dismiss the employee if it concludes that the employee's underlying misconduct justifies it.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is certainly best practice to prepare a terms of reference or scoping document before commencing an internal investigation. Ideally, it would cover the following:

- the matters to be investigated, including the limits of the investigation, and what is outside its scope;
- the purpose of the investigation, including (if applicable) whether it is for the purposes of providing legal advice to the organisation or if proceedings may be in contemplation;
- who will be conducting the investigation;
- the process the investigators will follow;
- the relevant internal rules, codes, policies and procedures that will govern the investigation;
- whether the investigation will include interviews and, if so, a general description of who might be interviewed;
- whether interviewees will be given copies of their interview transcripts;
- the predicted time frame for the investigation, with the caveat that it may be extended;
- that the role of the investigators is not the same as the role of the decision maker – that the investigators' role is to determine the facts, not outcomes;
- make clear that any interviewee can have a support person or representative in interviews at any time in the process;
- the type of report that will be produced at the end of the process, and to whom it will be disclosed; and
- the manager within the organisation who is responsible for the investigation and, if different, the contact person.

© Law Business Research 2021

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

The key steps would include:
- to take legal advice, particularly around the issue of preserving privilege over subsequent communications made by the company;
- to ensure that company document preservation procedures are executed;
- to consider public disclosure obligations;
- to consider the extent to which employees who may be involved should be suspended;
- to make any necessary insurance notifications; and
- to determine what investigative steps are required.

Although there may be no specific legal or ethical internal obligations on the company, it is likely to be a personal duty on company directors to ensure that those charged with governance are aware of material issues (of which a company director should reasonably be aware).

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

A company should co-operate with law enforcement and take the necessary steps to provide those documents captured by the wording of the notice, having reviewed documents for those protected by privilege. The company should review document preservation and destruction procedures to ensure that related material is preserved in the event that law enforcement make subsequent requests.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

The New Zealand Exchange Listing Rules (which apply to companies listed on the New Zealand Exchange (NZX)) require disclosure of 'material information' promptly and without delay (NZX Listing Rules (10 December 2020), Rule 3.1.1). The Rules also provide a number of exceptions, however, including where the information contains 'matters of supposition or is insufficiently definite to warrant disclosure', is generated for internal management purposes, or is confidential (Rule 3.1.2). It will therefore be a matter of judgement at what point a company should make this disclosure. There are no similar disclosure rules for private companies.

37 How are internal investigations viewed by local enforcement bodies in your country?

Local enforcement bodies have no objection to internal investigations, but may raise concerns if an internal investigation has the potential to interfere with their own

© Law Business Research 2021

investigation and evidence gathering. There are no particular statutory requirements as to how a company should conduct an internal investigation.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

In general, the attorney–client privilege applies to all types of dealings between lawyers and clients. The associated duty of confidentiality owed by lawyers is enshrined in the Lawyers and Conveyancers Act 2006.

The attorney–client privilege can also be claimed in relation to parts of an investigation conducted by lawyers and involving legal advice, or an investigation conducted for the dominant purpose of preparing for contemplated legal proceedings. Whether privilege can be claimed depends on the circumstances and a company should seek legal advice before commencing an internal investigation. Where privilege does apply, companies should keep relevant communications or work confidential to preserve privilege.

However, there are some statutory exceptions and disclosure obligations that take precedence over the attorney–client privilege. These exceptions tend to arise in connection with potential criminal activity or dishonesty; for example:

- where an otherwise privileged communication was produced for a dishonest purpose or for the purpose of planning to commit a criminal offence, a search warrant can be issued for disclosure of that document or communication;
- the Serious Fraud Office can require certain information about the location of a client, purely financial documentation or trust account records to be disclosed;
- in relation to the recovery of proceeds of crime, privilege cannot be claimed over communications made or brought into existence for the purpose of committing or furthering the commission of an illegal or wrongful act. Similar to the case of fraud, the Commissioner of Police can require disclosure of certain information about a client. No privilege attaches to purely financial documents;
- the Commissioner of Inland Revenue can require disclosure of some information in relation to a client's tax affairs in certain circumstances. Privilege again does not attach if a communication was made or brought into existence for the purpose of committing or furthering the commission of an illegal or wrongful act, or to purely financial documents;
- customs officers have similar powers to compel the production of documents and records. Privilege does not apply where a communication was made or brought into existence for the purpose of committing or furthering the commission of an illegal or wrongful act, or to purely financial documents; and
- in the context of anti-money laundering and counter financing of terrorism, a communication is not privileged if it is made, received, compiled or prepared for a dishonest purpose or to enable or aid the commission of an offence. Trust account records are also not privileged documents in this situation.

© Law Business Research 2021

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The Evidence Act 2006 codifies the law relating to privilege. The attorney–client privilege applies equally and in the same manner to individuals and corporations. The client is the holder of privilege.

Privilege attaches to communications between a person (which includes a corporation) and their legal adviser if:

- the communication was intended to be confidential; and
- it was made in the course of, and for the purpose of the person requesting or obtaining professional legal services from the legal adviser, or the legal adviser giving these services to the person.

Privilege may also attach, in defined circumstances, to communications or information where it is for the dominant purpose of preparing for a proceeding or an apprehended proceeding. This is known in New Zealand as litigation privilege. Communication with witnesses and expert reports is commonly covered by this type of privilege.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege applies to in-house counsel, provided they hold a current practising certificate in New Zealand. It is important to note that meeting the relevant criteria to invoke privilege in part of a communication or document does not automatically attach privilege to the whole communication or document.

In general, the privilege also applies to legal practitioners from overseas jurisdictions who are entitled to practise work equivalent to that of a lawyer or patent attorney in New Zealand.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The scope of the attorney-client privilege is likely broad enough to cover these situations.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There is no formal recognition for waiver as a co-operative step in law or policy. There is no situation in which a person under investigation is required to waive privilege to obtain co-operation credit.

© Law Business Research 2021

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Limited waiver of privilege exists in New Zealand. In the leading case of *B v. Auckland District Law Society* ([2003] UKPC 38, [2003] NZLR 326 (PC) at [68], citing *R v. Bain* [2008] NZCA 585 at [80]), the Privy Council noted:

> *It must often be in the interests of the administration of justice that a partial or limited waiver of privilege should be made by a party who would not contemplate anything which might cause privilege to be lost, and it would be most undesirable if the law could not accommodate it.*
>
> *The scope of limited waiver appears to be wide. The Court of Appeal has held that there may be situations where privileged material may even be referred to in court and produced in evidence without a general loss of privilege. But, it went on to say that a party who wishes to make only a limited waiver of privilege should make clear that the waiver is limited and take steps to ensure that the loss of confidentiality in the material is confined to what is necessary for the purposes of the limited waiver.*

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There seems no reason in principle why not.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists in New Zealand. It applies in respect of a document over which another class of privilege exists, and it protects the privilege holder against waiving the privilege in disclosing the document to another party who shares a common interest in the subject matter of the document or the relevant litigation. Common interest privilege only applies to the extent that a genuine common interest exists. If a disclosed document contains information in which the parties have no common interest, there is a risk that privilege has been waived in respect of that information. To avoid waiving the privilege, material must be kept confidential as between the parties with a common interest.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

In general, privilege is unlikely to attach to assistance given by third parties to lawyers. In some circumstances, a third party could be considered an agent of the client and invoke privilege in that way. Otherwise, only litigation privilege could potentially apply.

© Law Business Research 2021

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, witness interviews routinely form part of internal investigations. Interviews must be conducted in accordance with the rights of individuals, including employment rights. The corporation conducting the interview should be clear with the witness about the purpose of the interview and what the information will be used for. Generally, witnesses should not be anonymous or able to make off-the-record comments.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

New Zealand law recognises various categories of privilege, including legal professional privilege (or solicitor–client privilege) and litigation privilege, which may enable a privilege holder to withhold documents they would otherwise be obliged to disclose. How these privileges apply to witness interviews will be context specific, but there are good arguments that legal professional privilege will attach.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Employers have a duty to act in good faith towards existing employees. In conducting a witness interview, an employer must act in a way that is fair and reasonable. New Zealand's Employment Relations Act 2000 imports additional duties in circumstances where an employer is meeting with an employee for a disciplinary purpose. Beyond these general duties, employers are not restrained in their approach to interviewing employees.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no standardised procedure for the conduct of an internal interview in New Zealand. Employees are entitled to have in attendance a support person and a legal adviser, but neither is formally required. In general, an interview will be conducted by putting documents to the witness and asking open-ended questions. With the witness's permission, the interviews will usually be recorded, either electronically or in writing.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Mandatory reporting of misconduct is a feature of some regulatory frameworks within New Zealand; for example:

- qualifying financial institutions are required to report suspicious transactions to the Commissioner of Police under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (section 40). Failure by a company to report in breach of a reporting obligation under this Act (section 100) attracts a penalty fine of up to NZ$5 million;
- the Financial Markets Supervisors Act 2011 creates a supervisory scheme over issuers of debt securities. Under the Financial Markets Conduct Act 2013 (sections 116 and 118), an issuer of debt securities is required to report certain issues to its supervisor, including any contravention (or possible contravention) of its issuer obligations and any serious financial problems; and
- some professional regulatory bodies, such as the Teaching Council, the Medical Council and the Law Society, require mandatory reporting of certain misconduct or suspected misconduct in breach of particular codes of conduct relevant to the regulated profession.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The nature of an issue and the likely consequences of that issue (both with and without self-reporting) are the primary considerations relevant to a corporation's management and response. Where an enforcement outcome is likely, co-operation (including voluntary disclosure) routinely attracts a significant discount in mitigation. However, it is unusual for self-reporting or co-operation to result in a complete avoidance or immunity from liability. A punitive outcome and the associated reputational risk is likely regardless.

Within particular regulatory frameworks, New Zealand has taken steps to strengthen the incentive to self-report. The most relevant example is the Commerce Commission's Cartel Leniency and Immunity Policy (the Leniency Policy). In 2021, New Zealand criminalised cartel conduct. The Leniency Policy replicates immunity policies implemented in other jurisdictions, encouraging reporting by offering conditional immunity to the first participant in cartel conduct that reports to the Commission and provides evidence.

Where an incentive to self-report has cross-jurisdictional application, such as the Leniency Policy, that factor is relevant to a corporation's assessment of whether or not to self-report internationally.

© Law Business Research 2021

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The practical steps required to self-report misconduct to law enforcement vary depending on the type of misconduct and the area of regulation. In all instances, it is advisable to obtain independent legal advice prior to taking any further steps.

There are few practical restraints on the process of self-reporting. Regulatory agencies provide contact details for general reporting of misconduct or suspected misconduct. If misconduct is being reported pursuant to a particular scheme, such as the Commerce Commission's Leniency Policy, there are specific rules guiding the manner and nature of disclosure. Guidance is available on the Commerce Commission's website.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Most companies will co-operate with law enforcement after having received a notice requiring the production of documents. Law enforcers are usually highly responsive to responsible dialogue with a company through the case officer or assigned prosecutor. Section 57 of the Evidence Act 2006 provides a privilege for plea discussions, although a company must be a 'party to a criminal proceeding' before this privilege engages.

55 Are ongoing authority investigations subject to challenge before the courts?

Once an agency lays charges, a defendant can apply for a stay of these proceedings on the basis they are an abuse of process. However, because New Zealand courts have taken the view that prosecutions are acts of the executive with which they should rarely interfere, stays are unusual. The decision to prosecute is generally subject to judicial review, although some statutes providing powers of investigation expressly prohibit those powers being challenged in court (e.g., Serious Fraud Office Act 1990, section 20).

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

This decision calls for an assessment by the company of the benefit in agreeing consistent disclosure packages across all jurisdictions, against the burden to the New Zealand subsidiary of complying with a wide-ranging notice when it is unlikely that data stored in New Zealand will be a focus for a multi-jurisdictional investigation.

The cross-border data protection provisions in the Privacy Act 2020 are unlikely to apply in the context of mutual legal assistance requests. But a New Zealand company should consider them carefully before voluntarily disclosing material to overseas authorities.

© Law Business Research 2021

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The issue that arose in *R (KBR) v. SFO* ([2021] UKSC 2) has not directly been tested in New Zealand courts, and its determination would likely turn on the wording of the empowering statute in question. However, we believe that New Zealand courts would look to the extent to which the target of the notice had custody or control over the documents requested, rather than the location of the documents sought (see, e.g., Serious Fraud Office Act 1990, section 19).

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Yes. Mutual legal assistance requests are common. Requests for assistance in criminal investigations may be made to New Zealand by certain countries under the Mutual Assistance in Criminal Matters Act 1992 (section 24 sets out which countries are eligible to make a request for assistance). Requests by those countries will need to outline the nature and purpose of the assistance being sought, along with specified documentation and details (section 26). Requests can be refused by New Zealand at the discretion of the Attorney General, although section 27 of the Act sets out an apparently exhaustive list of factors which can justify refusal. Examples of types of assistance provided for by the Act include assistance in obtaining evidence in New Zealand (section 31), assistance in arranging for a person to give evidence or assistance (in relation to a criminal matter) in a foreign country (section 37), and assistance in obtaining articles by search and seizure (section 43).

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Yes. Section 36 of the Serious Fraud Office Act 1990, for example, requires every member of the Serious Fraud Office to observe the 'strictest secrecy' in relation to information obtained in the course of an investigation, subject to some exceptions.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Our advice would be to resist production, at least in the first instance, on the grounds that the documents are not within the company's control, insofar as the request requires the company to breach the foreign law to produce them.

© Law Business Research 2021

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

No. There are no blocking statutes in New Zealand.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Risks lie in the form of breaches of the Privacy Act 2020, banking secrecy obligations, or other contractual obligations of confidence for voluntary disclosures of information where a company would have a defence if compelled to make the production by law.

A degree of confidentiality attaches to information provided to law enforcement. Section 36 of the Serious Fraud Office Act 1990, for example, requires every member of the Serious Fraud Office to observe the 'strictest secrecy' in relation to information obtained in the course of an investigation, subject to some exceptions. The Official Information Act 1982 – the statute by which a person may obtain information held by government – has a number of carve-outs that could apply in the context of a request for investigatory materials (sections 6 and 9).

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies and their officers and employees can face both criminal and civil penalties, depending on the type and seriousness of the misconduct.

In practice, criminal prosecutions tend to be brought against directors and senior officers within an organisation. This could be because attribution of conduct to the company is challenging, or because the company itself is a victim of the wrongdoing.

In some situations, both the company and its senior officers can be prosecuted. A current example is the ongoing prosecution by WorkSafe (which monitors health and safety compliance) of 13 defendants for alleged health and safety failures which led to the deaths of 22 people and severe injury of a number of others when the Whakaari/White Island volcano erupted in 2019. Among the defendants, WorkSafe is prosecuting a tour company as well as its three owner-directors. The owner-directors are charged with alleged failures of due diligence duties; their company is alleged to have failed its duties to staff and tourist customers to provide adequate means of evacuation from the island.

A company, within the definition of 'person' in the Crimes Act 1961, can theoretically commit any offence that an individual can. Individuals will face imprisonment or pecuniary penalties (or both), whereas corporations tend to be subject to pecuniary penalties only.

There are specific criminal offences directed towards companies, including for non-compliance with statutory duties relating to corporate governance (Companies Act 1993, section 393) and disclosure (Commerce Act 1993, sections 86B and 87B), cartel behaviour (restrictive trade practices) (Commerce Act 1986, part 6), breach of duties relating to health and safety in the workplace (Health and Safety at Work Act 2015,

© Law Business Research 2021

part 2), failure to comply with reporting obligations (Financial Reporting Act 2013, sections 36H and 36Q), fraud (Companies Act 1993, sections 380 and 383; Serious Fraud Office Act 1990, sections 45 to 47), misleading or deceptive conduct (Financial Markets Conduct Act 2013; Fair Trading Act 1986), and failure to comply with licensing rules on entities that carry on business borrowing, lending or provide financial services (Non-Bank Deposit Takers Act 2013, section 11; Financial Markets Supervisors Act 2011, section 43). All can result in criminal conviction and penalty, and some can alternatively incur civil penalties.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

A company can have its registration suspended or cancelled by the Companies Office as a punishment for serious breaches of the law. The effect is that the company can no longer carry on business in New Zealand. The Companies Office also has the ability to remove an overseas company from an overseas register, where certain requirements are met (Companies Act 1993, section 341).

65 What do the authorities in your country take into account when fixing penalties?

When considering the appropriate penalty to impose, authorities will generally take into account the seriousness of any offending, the level of intent behind the offending, and any efforts to rectify the wrongdoing or make amends.

Criminal sentencing is governed by the Sentencing Act 2002, which sets out mandatory and discretionary factors a court should take into account when imposing a criminal sentence. In accordance with the Court of Appeal judgment in *R v. Moses* ([2020] 3 NZLR 583 (CA)), courts will first set a starting point based on aggravating and mitigating features of the offending, and adjust that starting point for aggravating and mitigating features of the offender (including any guilty plea).

Civil penalties are imposed in a similar way, and by reference to statutory requirements and comparable cases for the particular misconduct.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

New Zealand does not have non-prosecution or deferred prosecution agreements per se. However, 'enforceable undertakings' can be entered into with particular enforcement agencies in lieu of prosecution, such as WorkSafe (which monitors health and safety compliance), the Department of Internal Affairs, the Commerce Commission and the Financial Markets Authority. Some agencies have formal policies, while others may consider enforceable undertakings on a discretionary basis.

In general, enforcement agencies are likely to look at the seriousness of the conduct, the company's history of compliance, and whether an enforceable undertaking is in the

© Law Business Research 2021

public interest or provides benefits to a relevant industry or community (drawing on a few guiding principles in the WorkSafe policy). However, if a company breaches an enforceable undertaking, there is nothing to prevent a prosecution from being reinitiated.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

A company may apply to a court for suppression in connection with a criminal proceeding under the Criminal Procedure Act 2011, or to an enforcement agency where that agency has power to make non-publication orders (such as the Financial Markets Authority (Financial Markets Authority Act 2011, section 44) and the Commerce Commission (Commerce Act 1986, section 100)).

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Settlement does not preclude a public court judgment or a finding of liability. Settlement in the New Zealand context is unlikely to involve paying money to avoid prosecution. Even where a defendant company and the prosecuting agency support the imposition of an agreed penalty, a court will need to give public judgment for that penalty to have effect. The courts can also disagree with and disregard the agreement reached by the parties if it comes to a different conclusion on the appropriate penalty.

When considering settlement with an enforcement authority, it is important to carefully consider whether liability is being admitted. Criminal conviction can affect a company's ability to access public funding and registration in certain sectors.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

New Zealand does not typically use external corporate compliance monitors.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private actions can run in parallel to regulatory prosecutions. Any member of the public may be entitled to and can apply for access to certain 'official information' held by government departments, pursuant to the Official Information Act 1982, although there are a number of carve-outs for sensitive investigatory material.

Parties to private actions might be able to apply to enforcement or regulatory agencies to obtain further information from an investigation, but there are likely to be confidentiality or secrecy considerations particular to a given agency, especially when an investigation is still in progress.

© Law Business Research 2021

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In general, there is no rule preventing the media from reporting that an investigation is under way; however, publicity is managed carefully at the investigatory stage of a potential case. Participants in an investigation are unlikely to comment publicly while an investigation is under way. Under the Contempt of Court Act 2019, any person (including the media) can be found liable for an offence if a publication interferes with the administration of justice (for example, by causing a real risk to a defendant's right to a fair trial or by undermining public confidence in the independence, integrity, impartiality or authority of the judiciary).

Once a matter is before the courts, the media have significant rights to access court and report on proceedings.

Proceedings are generally heard in open court. However, public access may be restricted where required in the interests of justice, for example, in sensitive cases or when a witness protection issue arises (Criminal Procedure Act 2011, section 197). In such cases, members of the media may be granted access to closed court proceedings in recognition of their role as the eyes and ears of the public (Criminal Procedure Act, section 198).

The publication of certain details of a criminal case are automatically suppressed under criminal procedure legislation (e.g., under Criminal Procedure Act 2011, sections 199A, 203 and 204). In addition, the court can order that further details of a case be suppressed temporarily or permanently (e.g., under Criminal Procedure Act 2011, sections 199C, 200 and 202). Members of the media have the right to be heard on the issue of suppression (Criminal Procedure Act 2011, section 210).

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There is no uniform approach to the management of corporate communications – corporations make their own determinations about the management of publicity and public relations. Public relations firms exist and it is not unusual for a firm to be engaged to advise on the management of any publicity, including in relation to a corporate crisis. Even where such assistance is engaged, most commonly, the chief executive officer or managing director of a corporation will front any matter of publicity.

73 How is publicity managed when there are ongoing related proceedings?

The management of publicity is a matter for the corporation, usually in reliance on legal and public relations advice. Most often, corporations will decline to comment while an investigation or proceeding is under way or will limit any comment to simply confirming the existence of the investigation or proceeding. Once an outcome has been determined, corporations may release a prepared statement to the media for publication.

© Law Business Research 2021

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

The New Zealand Exchange (NZX) listing rules provide the general rule that a listed issuer must disclose material information to the market. However, there are exceptions to this rule, including where the information contains an incomplete proposal or negotiation, or the information is confidential and its confidentiality is reasonably maintained (NZX Guidance Note on Continuous Disclosure (10 December 2020)).

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

ESG governance and regulation is a relatively new frontier in New Zealand but one which is increasingly important to public policy on corporate governance.

New Zealand has an Emissions Trading Scheme that aims to reduce greenhouse gas emissions across emissions-intensive and trade-exposed industries. The Scheme requires certain businesses to measure and report on their greenhouse gas emissions and requires some businesses to buy and surrender to the government one emissions 'unit' (NZU) for each tonne of emissions they produce. NZUs (also known as carbon credits) are supplied to the market for business to buy and sell between each other.

The New Zealand Exchange (NZX) promotes disclosure of ESG matters but does not yet regulate it. The most recent NZX Corporate Governance Code, released in 2017, framed one of its recommendations (Recommendation 4.3) to issuers on disclosure of ESG:

> *Financial reporting should be balanced, clear and objective. An issuer should provide non-financial disclosure at least annually, including considering environmental, economic and social sustainability factors and practices. It should explain how operational or non-financial targets are measured. Non-financial targets should be informative and include forward looking assessment and align with key strategies and metrics monitored by the Board.*

The NZX has also published an ESG Guidance Note to encourage ESG reporting.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

The government intends to introduce a mandatory climate-related disclosures regime, which would come into force in 2022, with first disclosures to be made in 2023. The Financial Sector (Climate-related Disclosures and Other Matters) Amendment Bill is currently going through Parliament and is expected to pass. The disclosure regime will apply to certain large financial sector organisations, including some overseas incorporated organisations, and will require disclosure in compliance with standards issued in accordance with the recommendations of the G20 Task Force on Climate-related Financial Disclosures.

© Law Business Research 2021

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

There has not been any ESG-related litigation or enforcement activity to date, but it is expected once mandatory climate-related disclosures come into force. The Ministry of Business, Innovation and Employment suggests that consideration of ESG factors may even be within the remit of fiduciary duties owed by company directors.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

There is the possibility of the introduction of a new whistleblowing law, a new autonomous sanctions law and a new climate-related disclosures law. Moreover, the Privacy Commissioner is likely to expand the exercise of its new compliance powers under the Privacy Act 2020. Further, we anticipate the prosecution and regulation of money laundering and terrorism financing to increase markedly following the Financial Action Task Force's 2021 Mutual Evaluation Report, which highlighted a number of possible improvements in the New Zealand money laundering regime.

© Law Business Research 2021

18

Peru

Alberto Rebaza, Augusto Loli, Héctor Gadea, María Haydée Zegarra and Sergio Mattos[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The most relevant criminal investigations still relate to *Operation Car Wash*, in which Brazilian construction companies are alleged to have bribed Peruvian public officials to have infrastructure work contracts awarded at inflated prices.

2 Outline the legal framework for corporate liability in your country.

Statute No. 30424 (the law regulating the administrative liability of corporations, in force as of 1 January 2018) and its Regulation (Supreme Decree No. 002-2019-JUS) establish the liability of corporations for collusion crimes, domestic and transnational bribery, influence peddling, money laundering and funding of terrorism. In this sense, if an individual linked to a corporation commits any of these crimes, either in the corporation's name or on behalf of the corporation and to its benefit, whether directly or indirectly, the corporation could be liable for the crime autonomously. However, if the corporation proves that, before the crime was committed, it had an effective criminal compliance programme in place, it could expect immunity from sanctions or a reduced sanction. In March 2021, the Superintendency of the Securities Market (SMV) issued guidelines to be considered when assessing the implementation and operation of criminal compliance programmes.

1 Alberto Rebaza is managing partner, Augusto Loli, Héctor Gadea and María Haydée Zegarra are partners and Sergio Mattos is a senior associate at Rebaza, Alcázar & De Las Casas.

© Law Business Research 2021

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Regarding the autonomous liability of corporations foreseen in Statute No. 30424, an investigation will be carried out by a prosecutor, which requires the intervention of the SMV to issue a technical report regarding the effectiveness of the compliance model of the company being investigated. If the compliance model is not appropriate, the prosecutor could take the company to trial, at which a criminal judge could impose sanctions.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The Supreme Court has established that to initiate a preliminary investigation, only a 'simple initial suspicion' is required, which in turn constitutes 'the least intensive degree of suspicion'.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

For these cases and others in which the investigated party considers that his or her rights are not being respected, or that he or she is being subjected to illegal requirements (e.g., fishing expeditions), a motion may be filed with the preliminary investigation judge, who may invalidate the subpoena or limit its scope.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Originally, the Code of Criminal Procedure regulated only effective co-operation for natural persons. Depending on the relevance of the information provided, a prosecutor may request a criminal judge to exonerate or reduce the sanction.

Statute No. 30737 (passed on 12 March 2018) modified the Code of Criminal Procedure and now companies are allowed to enter into co-operative agreements with the prosecutor. In exchange for providing relevant, verifiable and timely information to clarify the facts being investigated and to prosecute the natural persons involved, the companies may obtain an exemption or reduction of the sanction.

Likewise, the clemency proceeding established in Legislative Decree No. 1034 (Law of repression of anticompetitive behaviour, of 25 June 2008) allows those who violate the competition rules to be exonerated from an administrative sanction or to mitigate its magnitude if they provide evidence that helps to detect and prove the existence of collusion (i.e., a cartel) and to sanction the liable parties.

© Law Business Research 2021

7 What are the top priorities for your country's law enforcement authorities?

Authorities focus their efforts on the investigation of emblematic corruption or money laundering, which, in some cases, involve the political and business elite. For instance, former presidents, political parties that have participated in presidential campaigns, and construction companies and their directors, among others, are being investigated for the aforementioned crimes. Further, the Prosecutor Office is currently investigating corruption allegations relating to public procurement purchases and bids in the context of the covid-19 pandemic.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

From a law enforcement authority perspective, it is important that a company being investigated under Statute No. 30424 has an effective compliance programme in place before an offence is committed if the legal entity intends to obtain immunity or a reduced sanction. Under Article 17 of this Statute, an effective compliance programme must be appropriate to the nature, risks, needs and characteristics of the company. As a result, the Regulation of Statute No. 30424 establishes that the first step to designing and implementing a compliance programme must be an assessment of the company's risk profile. In this context, the Regulation also states that the minimum elements of a compliance programme are:

- a thorough risk assessment and controls;
- an in-house compliance officer;
- a whistleblowing hotline and complaints procedures;
- periodical training; and
- continuous monitoring and assessment of the compliance programme.

The guidelines issued by the SMV are a reference framework to assess whether the elements listed above have been adequately implemented. Further, based on our experience, for a company's compliance programme to work efficiently, it is essential that there is a true 'tone at the top', reflected, for example, by providing autonomy and sufficient resources to the compliance officer. In addition, to the extent that is appropriate for the particular company, lawyers are advised to follow the standards outlined in the updated guidelines for Evaluation of Corporate Compliance Programs, published by the US Department of Justice Criminal Division.

Regarding anticompetitive matters, on 3 June 2020, the National Institute for the Defence of Competition and Intellectual Property (Indecopi) published a guide to antitrust compliance programmes.

© Law Business Research 2021

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

The National Cybersecurity Policy of 2017 is applicable to public administration entities. The main aspects of this Policy are (1) to protect the information, data and state information infrastructure and the technology used for processing the same from internal or external threats, whether deliberate or accidental, to ensure the confidentiality, integrity, availability, legality and reliability of the information, and (2) to ensure the implementation of legislative proposals and regulations relating to information security or cybersecurity.

Statute No. 30999 (Cyber Defence Law, published on 27 August 2019) establishes the regulations framework on cyber defence of Peru, regulating the military operations in and through the cyberspace executed by bodies that are part of the Ministry of Defence within their scope of competence. The purpose of this regulation is to defend and protect the sovereignty, national interests, national critical assets and key resources to maintain the nation's capacity to face threats or attacks in and through cyberspace insofar as they affect national security.

Since the legislation is relatively recent, there is still no case law.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Statute No. 30096 (Law of Computer Crimes, published on 22 October 2013) sanctions behaviour such as illegal access and attacks on the integrity of computer systems (hacking), propositions with sexual purposes to underage children through technological means and computer fraud, among other things. In January 2021, the Prosecutor's Office ordered the formation of a Specialist Cybercrime Prosecution Unit.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Article 2 of the Criminal Code establishes a general rule that Peruvian law applies to a crime committed abroad, when:

- the person committing the crime is a Peruvian public official or worker fulfilling the duties of his or her office;
- public security or peace are attacked, or the incident involves money laundering, provided the effects of the incident occur in Peru;
- the act or behaviour offends the Peruvian state and national defence, the powers of the state or constitutional order, or the monetary order;
- the act or behaviour is committed against a Peruvian or by a Peruvian and the crime is foreseen as susceptible to extradition pursuant to Peruvian law, provided it is also

© Law Business Research 2021

punishable in the state where it was committed and the agent enters Peru in any way; or
- Peru is obliged to repress the behaviour according to international treaties.

In turn, Article 397-A of the Peruvian Criminal Code sanctions any person who offers, grants or promotes bribery, directly or indirectly, to foreign officials in exchange for obtaining a particular advantage for himself or herself or for others within the framework of international economic or trade activities (transnational bribery).

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

In such investigations, one of the main challenges is the time it takes to process the official communications with the authorities of other countries, for example, for international judicial assistance. However, in respect of the emblematic cases, such as *Operation Car Wash*, the delay in replies and effective assistance by foreign authorities has been considerably reduced.

Owing to the free transit restrictions imposed during the covid-19 pandemic, prosecutors started to conduct witness interviews through digital platforms. Currently, most depositions are conducted in this manner.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Under the protection of Article 6(c) of the Code of Criminal Procedure, the *non bis in idem* principle or *res judicata* is applicable if there is the intention of criminally investigating a company in Peru for deeds that have previously been subjected to a final decision by a foreign authority against the same company.

If a company is being investigated both administratively and criminally for the same deeds and on the same grounds, by virtue of Article III of the Preliminary Title of the Code of Criminal Procedure, the criminal jurisdiction prevails over the administrative one. Other than this, there is no institution that is analogous to the US 'anti-piling on' policy.

14 Are 'global' settlements common in your country? What are the practical considerations?

There is no record of any global settlement, nor any specific regulation of the matter.

© Law Business Research 2021

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Matters investigated in another country that could have an effect in Peru can be considered as evidence to initiate a criminal investigation. Likewise, the authorities may initiate a judicial co-operation agreement with foreign authorities to share relevant information and evidence. For example, this has been happening in *Operation Car Wash* with the information provided by the Brazilian authorities.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The Peruvian government has not imposed economic sanctions against foreign countries, governments, entities or people who may represent a threat to the interests of Peru or of the international community.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Peru has not applied any economic sanctions.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Not applicable.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

There is no blocking legislation in Peru.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

There is no blocking legislation in Peru.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Misconduct usually arises through media reports, internal audits and, in those companies supervised by a financial intelligence unit (companies within the financial system, mining

© Law Business Research 2021

activity, construction, etc.), through reports of suspicious operations of money laundering to the regulator.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Statute No. 29733 (Law of Personal Data Protection, published on 3 July 2011) and its Regulation (Supreme Decree No. 003-2013-JUS) have the purpose of guaranteeing the fundamental right of protection of privacy. Companies are expected to provide appropriate treatment of the personal data of their clients, workers and other natural persons concerning their activity.

The titleholder of the personal data has the rights of information, updating, inclusion, correction, suppression, opposition, objective treatment, protection and of being indemnified. The National Authority for the Protection of Personal Data may sanction a company if it proves that it made any inappropriate use of personal data.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Peruvian Data Protection Authority has been issuing fines for non-compliance with the rules on personal data protection since 2015. The organisations that have been fined are of different types and include clinics, universities, banks and public entities. As an example, Google Inc was sanctioned in 2016 with a fine of US$75,000.

It is important to bear in mind that Peruvian data privacy rules are applicable not only to natural persons and legal entities established in Peru, but also to those using media located in the Peruvian territory.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

If an internal investigation entails sharing information with peers located abroad (for example, a parent company or law firm), the cross-border flow of information must be duly communicated to the national authority and comply with the legal provisions.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Although there is no rule that specifically regulates the control of work tools (email, cell phones, etc.) by an employer, Article 2.10 of the Constitution establishes that every person has the right to secrecy and to the inviolability of communications and private documents.

The Constitutional Tribunal (Docket Nos. 114-2011-PA/TA, 3599-2010-PA/TC and 05532-2014-PA/TC) and the Supreme Court (Cassation No. 14614-2016-Lima) have established, from a labour point of view, that an employer is forbidden to inspect the use of corporate email assigned to its employees, unless it has the express authorisation of

© Law Business Research 2021

the employees every time the employer wants to log in to view the email. Thus, a general waiver signed by an employee when joining the company will not be sufficient.

However, in the criminal sphere (Nullity Appeal No. 817-2016/Lima), the Supreme Court established that if there is a high probability that corporate email has been used to exchange communications with criminal content, it is not illegal or unconstitutional for the employer to inspect its employees' email for the purposes of a criminal claim. A prosecutor may subsequently use the email as admissible evidence in a criminal procedure.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants are used frequently by prosecutors, particularly in emblematic investigations for corruption or money laundering crimes, such as *Operation Car Wash*.

According to Article 214° of the Code of Criminal Procedure, a search can be carried out when it is reasonable to consider that evidence may be found inside the premises subject to the search. Authorisation by a judge is required.

Both the search and the seizure of documents must be limited to what has been authorised by the judge. There is a possibility of controlling a warrant dictated by a judge through an appeal in which the pertinence, proportionality and reasonableness of the measure are discussed. However, even if the search is considered legal, the judge can be asked to exclude privileged material and any documents not related to the investigation.

Note that, in the administrative field, the regulation of the powers, rules and organisation of the National Institute for the Defence of Competition and Intellectual Property (Indecopi) (under Article 2 of Legislative Decree No. 807) allows unannounced visits – not searches – during a proceeding. If a company denies access to the authority, a judicial mandate will be required.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privileged material cannot be seized during a search ordered by a judge and carried out by a prosecutor. In this sense, it is recommended that all materials or reports of this nature be labelled as 'protected under professional secrecy', in accordance with the procedure established in Article 2.18° of the Constitution, Article 30° of the Attorney's Code of Ethics and Article 165° of the Criminal Code. Moreover, the presence of an external lawyer is recommended during a search to enforce privilege over documents having such a condition. The Supreme Court has ruled that 'the right to professional secrecy must prevail over the right to obtain evidence' (Cassation No. 272-2016-Tacna, fj.13).

© Law Business Research 2021

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

As investigated parties, people are not compelled to testify. They have the right to remain silent, and silence cannot be treated negatively. As witnesses, however, people are compelled to testify. Nevertheless, there is the possibility of opposing the testimony under certain specific circumstances, such as the fact that questions may refer to the witness's own criminal liability, that the investigated party is a close relative or that the questioning is about some type of professional secrecy or state secret.

Moreover, investigated parties are not compelled to collaborate with their own prosecution.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There are no specific financial incentives for whistleblowers in criminal procedures. However, Article 39° of the Regulation of Statute No. 30424 establishes that companies must adopt protection measures to avoid retaliation against the people that use a whistleblowing channel.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

During the process of an internal investigation, 'non-specific labour rights' are applicable. This relates to actions, the legal entitlement and enforceability, of which goes beyond the standard entitlements of workers (as set forth in the Constitution), such as presumption of innocence, due process, right of defence, right to intimacy, right to secrecy and inviolability of communications, among other things.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

All employees have the same rights during the term of an employment contract. During an investigation, the employer cannot adopt any type of preventive measure (for example, suspension of the contract), unless he or she has the employee's consent. The only exception to this rule is foreseen for cases of sexual harassment, in which the employer is entitled to suspend – or transfer to another workplace – the alleged harasser to protect the victim.

© Law Business Research 2021

Without prejudice to the foregoing, in practice employers usually grant paid leave unilaterally to employees involved in an investigation. Notwithstanding the foregoing, this practice could be questioned, alleging an affectation to the right to 'effective occupation'.

Finally, the employer may adopt disciplinary measures when he or she indubitably verifies that an employee has engaged in labour misconduct or irregularity. If a dismissal proceeding is initiated, the employee must be notified in a letter of the facts that constitute the serious offence that may lead to his or her dismissal.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

As a general rule, an employee should volunteer or give his or her consent to participate in an investigation.

However, the seriousness of the investigated deeds and how they relate to the position of the employee could mean a failure to comply with the labour obligations if he or she refused to collaborate during an investigation process. In such a situation, we consider that this would constitute an assumption of a violation of good faith. In this situation, the employer may impose reasonable and proportionate disciplinary measures (i.e., warning, suspension or even dismissal).

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is not a common practice. However, it is recommended that at the commencement of each internal investigation, a document be prepared that defines its objectives and scope. Likewise, among other aspects to prioritise, the hypothesis of the investigation, the team in charge of the investigation and the means of proof to be used should be defined, as well as the fact that, owing to the nature or complexity of the investigated deeds, external advice will be required, both legal and regarding public relations.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no legal obligation for companies to report dishonest behaviour that has occurred. However, once an internal investigation has commenced, the company must try to remedy or compensate the damage caused, and identify and correct any internal proceeding the failure of which originated the dishonest behaviour, particularly any action relating to the compliance model. Likewise, according to Article 38° of the Regulation of Statute No. 30424, the internal investigation and subsequent self-reporting could be taken as a sign of an effective compliance model and, therefore, could release the company from liability.

© Law Business Research 2021

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is advisable for a company to have a protocol to address such requests satisfactorily and in which the following steps are established:

- identification of the events that have brought about the authority's request, in collaboration with the company's legal department or external legal advisers;
- verification of the validity of the authority's request, that is to say it is not violating any fundamental right such as due process, professional secrecy or protection of personal data;
- informing the competent authority if the information is in the hands of third parties or if it requires a third party's authorisation to be submitted;
- a detailed review of the information, prior to submission, to identify any legal contingency that could arise from it;
- designing a defence strategy, both from a legal and a communication point of view, to mitigate the contingencies that could be generated by the submission of information; and
- if, because of receiving a notice or subpoena, a company becomes aware of any dishonest behaviour within the company, an internal investigation must be commenced to establish its scope.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is no obligation to publicly disclose the existence of an internal investigation. However, at the moment of deciding whether to disclose this information, companies must take the following factors into consideration:

- the degree of probability that the prosecutor or another authority becomes aware of the facts that are the subject matter of the investigation;
- the existence of an internal investigation may demonstrate to the authorities that the company itself, through its compliance model, identified, investigated and sanctioned dishonest behaviour; and
- by collaborating with the authorities in providing relevant information that allows clarification of the criminal deed, the company could be applying for an attenuation or exemption of the sanction.

37 How are internal investigations viewed by local enforcement bodies in your country?

Spontaneous internal investigation for suspicion of criminal wrongdoings is a tool that has only recently been available within the Peruvian corporate environment. There is still no case law about its real worth to the authorities. However, any form, or sign, of collaboration with the investigation is always well received by prosecutors.

© Law Business Research 2021

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Although there is no specific regulation in Peru, the attorney–client privilege could be claimed over the findings of an internal investigation in which an external attorney directly participated. In this sense, it is advisable that the instrument or document that initiates the investigation identifies the external attorneys who will participate and that their intervention is documented, for example, during the interviews and in the communications exchanged by the team in charge of the inquiry.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

According to the Code of Ethics of the Peruvian Bar Association, there is no distinction in the treatment of the attorney whether the client is a natural person or a corporation. In this sense, the scope of the attorney–client privilege is the same for both.

Likewise, in the framework of an internal investigation, to avoid the lawfulness of the gathered information or the scope of the attorney–client privilege being questioned, it is advisable to inform the parties at each stage of the investigation that the external attorney only represents the interests of the company; thus, the privilege will be between the attorney and the company and not between the attorney and the employee being interviewed.

The holder of the privilege is the client.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Although there is no specific regulation in Peru, based on the guidelines adopted by foreign courts (for example, in the European Court of Justice *Akzo Nobel Chemicals Ltd* case), certain Peruvian specialists consider that the attorney–client privilege applies only when external attorneys are involved.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

To the extent that the waiver to the privilege corresponds to the client, it would apply equally to the advice provided by both national and foreign external attorneys regarding an investigation carried out in Peru.

© Law Business Research 2021

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

In the framework of an effective collaboration, if a company wants to obtain a benefit that, in the best-case scenario, exempts it from liability, it is advisable to waive the attorney–client privilege, if necessary, to provide all the information required by the authorities. Waiver of this privilege is always voluntary.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no specific regulation in Peru. A company could waive privilege before the prosecutor and maintain privilege before third parties denying the production of the same information. However, law enforcement may share the information waived to other government agencies.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

The attorney–client privilege can be maintained in Peru after a limited waiver in another country. However, the information disclosed in another country may be shared with Peruvian authorities through international co-operation.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept does exist in Peru. If there are no conflicts of interest, the same attorney may represent several clients in the same criminal procedure.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

The attorney–client privilege extends to those who assist external attorneys, such as experts, accountants and translators, among others.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes. In turn, it is advisable that at each stage of an internal investigation, the external attorney announces that his or her intervention is on behalf of the company and not as an attorney of any internal witness.

© Law Business Research 2021

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

The parameters of the interviews within an internal investigation are not regulated in Peru. However, to avoid the admissibility of the gathered evidence being questioned in the event that the company decides to share it with the competent authority, it is advisable to inform the employee or third party before starting the interview that the attorney–client privilege applies to the company and not the employee or third party.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Although there is no predetermined protocol for conducting interviews, it is common for an attorney to participate in them as a representative of the company. Likewise, minutes are usually written, transcribing part of the information provided.

It is not common that employees have their own legal representation during interviews. However, if an employee does request that a lawyer attends, the employer should agree to the request to prevent the employee from alleging any coercion in making his or her statement.

While the covid-19 pandemic continues, internal interviews may be conducted via digital platforms with appropriate protocols and strict security measures in place to ensure confidentiality and legal privilege.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no legal obligation for companies to report misconduct to the authorities.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting is advisable when it is probable that a company may obtain a benefit in exchange for the information it provides and that the prosecutor may find out about the wrongdoing by other means. Self-reporting will be considered as evidence that a company's compliance programme was efficient, and the company could receive a reduced penalty or even an exemption from a penalty. If the decision to self-report has been made in Peru, it is advisable also to make the self-report in other countries that have jurisdiction to prosecute the crimes.

© Law Business Research 2021

53 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no express regulation on how to self-report. It is advisable that an external attorney seek an interview with the prosecutor to establish his or her interest in the matter. However, it is also advisable to delay arranging such an interview until after an internal investigation has established the actual scope of the misconduct, the persons involved and the legal, financial and reputational contingencies that could be activated.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

How a company should respond to a notice or subpoena will depend on the conditions under which it has been served. If the company is included as a defendant in an investigation, it is recommended that its attorneys review the case file held by the authorities before providing any kind of statement or information. However, if a company has been called only as a witness, its lawyers do not have the right to review the case file. Nevertheless, the company representative who has been called as a witness does have the constitutional right to be advised by an attorney during his or her testimony before the authorities.

In-house or external lawyers may have interviews with prosecutors to address their concerns, such as to clarify the scope of the subpoena and the deadline with which they must comply.

55 Are ongoing authority investigations subject to challenge before the courts?

Motions challenging investigations may be filed when the investigated deeds lack any criminal nature or when fundamental rights are violated, such as due process and the right to produce evidence, among other things.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Companies should address the local subpoena to the full extent regardless of the existence of a foreign subpoena. Local law enforcement authorities will not take into account the subpoenas issued by foreign authorities in making any alterations to the scope of their inquiry and will expect compliance with the local request. Therefore, companies should verify that the information provided to the different authorities, both domestic and foreign, is not contradictory.

© Law Business Research 2021

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The general rule is that the company must comply with the subpoena. However, if the scope is unreasonable or the costs to produce the material are prohibitive, a motion may be filed with the competent judge.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

There has been an increase in law enforcement co-operation with other countries as a result of *Operation Car Wash*. The Code of Criminal Procedure regulates the formalities that must be observed.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

A prosecutor's investigation is confidential. Only the investigated parties and the attorneys of the alleged victims may have access to it (note that in corruption or money laundering cases, the victim is represented by the state attorney). If the case reaches trial, which is public, the information may be disclosed.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A legal report from counsel in the foreign country should be obtained, explaining that the information may not be produced.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

There are some sectors in which statutes of secrecy exist, such as banking, tax reports and communications. If a foreign state requires this type of information, it must obtain an order from a Peruvian judge.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The confidentiality of the information or documentation provided to the authorities need only be maintained during the investigation phase. The information may be revealed at trial. Further, foreign regulators may seek the information produced through international co-operation channels.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The sanctions to companies imposed by a criminal judge are fines, temporary suspension of activities, cancellation of licences, debarments and, when a company has been incorporated and operated just to commit crimes, the dissolution of the company. A monitor can be appointed for up to two years. The natural persons, public and private officers can be sanctioned with imprisonment, fines and disgorgement. This is all without prejudice to repairing the generated damages that must be jointly and severally assumed by the natural persons and the company.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Peruvian courts have no jurisdiction to avoid companies resettling in another country. However, information about local wrongdoing may be shared to foreign authorities through international co-operation to enable suspensions or debarments.

65 What do the authorities in your country take into account when fixing penalties?

A judge will take into account the benefit the company has obtained or expects to obtain from committing the crime when imposing a fine, which is usually between twice and six times the amount of the benefit. If the benefit cannot be determined, the company's annual income will be taken into account by the judge to fix the fine.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Yes. For this purpose, a company must admit committing the crime, provide evidence against third parties (usually public officers) and remediate. In exchange, a company could obtain exonerations or reduced sanctions. If it is found that a company hid information

© Law Business Research 2021

or did not fully collaborate, the agreement can be reverted and the criminal proceedings may continue.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

The effective collaboration agreements are ruled precisely by secrecy from the beginning to the end of the investigation. The other investigated parties do not know the identity of the collaborator.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

The company should weigh the collateral effects of confessing to committing a crime, such as reputational and financial damage. Likewise, the company should take into account that its collaboration may result in members or former members of the company being sentenced to imprisonment.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Since January 2018, external monitors may be imposed for up to two years as a sanction by a judge. However, this measure has not been enforced to date.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private actions parallel to the criminal proceeding are allowed, as is a proceeding for reparation or indemnification for damages. However, if the injured party so desires it, that party can take on a civil action in the criminal proceeding and request civil reparation in the same criminal proceeding. In these circumstances, the party injured by the crime will have access to all the evidence in the criminal proceeding.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

The Code of Criminal Procedure establishes the prohibition of publishing the procedural actions during a prosecution investigation. However, the trial is public. There are certain exceptions, including when the sexual morality, the private life or the physical integrity of someone participating in the trial is affected, when national security is affected, or when a particular commercial or industrial secret is threatened.

© Law Business Research 2021

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There is no general rule, and a lawyer's recommendations will vary depending on the assessment of each case. Having said that, if the client is a large corporation and is facing a severe crisis in connection with a criminal investigation, it is always advisable to hire a public relations agency, which should work alongside the lawyers to assess both the accuracy and the strategic effects of the information provided to stakeholders and of public opinion. Further, the company's strategy should aim to stop the spread of news about any criminal involvement.

73 How is publicity managed when there are ongoing related proceedings?

Publicity depends on the degree of media coverage, or on the role of the company or the individual in society. The statements of a company under investigation must be short and not lead to speculation.

In Peru, confidential information about an investigation is usually leaked to the media when there is a case of public interest.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

It could be mandatory if the company in which the settlement has been agreed is a listed company and if the settlement, or the settled issue, is capable of having significant influence on the security of the company, its business, its financial situation or any other aspect that could be considered relevant by a reasonable investor, or that could alter the decision to sell, purchase or keep securities for a reasonable investor. If deemed mandatory, a reserved report could be made; thus the company will report the settlement to the regulator only. However, authorisation for such a report is at the regulator's discretion. Hence, if granted, full disclosure will not be required until the judge has approved the settlement.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

ESG is not specifically regulated under any legislation in Peru for its general application. However, there is some regulation for certain sectors that requires the application of ESG matters, such as the following acts and resolutions:

- Resolution 033-2015-SMV/01 (issued by the Superintendency of the Securities Market), which requires that listed companies shall disclose annual sustainability reports.
- Directive 068-2015/DE-FONAFE, whereby the National Holding Fund for State Enterprises (Fonafe) approved the Guidelines for Corporate Social Responsibility applicable to 32 state-owned companies that span the electric, financial, oil and gas industries, among others.

© Law Business Research 2021

- Resolution 1928-2015 (issued by the Banking and Insurance Superintendence), whereby the agency requires the application of the Equator Principles for loans of more than US$10 million granted to execute investment projects. The objective of this Resolution is to avoid exposing the financing system to social and environmental risks relating to the execution of said projects.

In addition, environmental regulation applicable to extractive sectors in Peru (i.e., mining, oil and gas, and electricity) requires the application of social indicators as part of the social responsibility programmes implemented by companies and included in their environmental assessments.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

The Lima Stock Exchange (BVL) has announced the incorporation of an ESG index in the local market by the end of 2021. This index will replace the current S&P/BVL IBGC Index (which measures only corporate governance aspects) and will incorporate the measurement of ESG aspects.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

There is no legislation that regulates litigation proceedings concerning ESG matters; hence, there is no case law.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

There is a legislative proposal to broaden the scope of application of Law No. 30424 so that legal persons are also criminally liable for the commission of the crime of prohibited financing of political parties. Likewise, there is another legislative proposal in which, although the Superintendency of the Securities Market would continue to carry out the technical assessment of criminal compliance programmes, it seeks to provide further powers to the Prosecutor's Office to carry out its own investigations to analyse the effectiveness of criminal compliance programmes.

© Law Business Research 2021

19

Poland

Marcin Ciemiński, Paweł Pogorzelski, Monika Diehl and Michał Magdziak[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Currently the highest-profile investigations in Poland concern various financial institutions. The scope of recent cases includes bond issuers, closed-end investment funds and banks.

Owing to very low enforcement actions concerning the criminal liability of corporations, the enforcement agencies are focusing primarily on the individual criminal liability of managers.

2 Outline the legal framework for corporate liability in your country.

The liability of corporate entities for criminal offences is regulated by the Act on the Criminal Liability of Collective Entities for Punishable Offences (the Liability Act). In general, under the Liability Act, a corporate entity may be liable if an offence mentioned in the Liability Act is committed by a specific person and that person's conduct has resulted, or may have resulted, in a benefit for the corporate entity.

The corporate entity will face liability for the actions of individuals only if its bodies or representatives have failed to exercise due diligence in preventing the commission of an offence, or if the entity has failed to exercise due diligence in hiring or supervising a person given permission to represent it. The lack of criminal liability of a corporate entity does not exclude the possibility of the corporate entity incurring civil liability for the damage caused or the administrative liability of the entity.

1 Marcin Ciemiński is a partner, Paweł Pogorzelski is a counsel, and Monika Diehl and Michał Magdziak are advocates at Clifford Chance.

© Law Business Research 2021

The maximum fine under the Liability Act is 5 million złotys (but cannot be higher than 3 per cent of the corporate entity's revenues generated in the year in which the offence was committed).

The Liability Act is considered inefficient and is rarely applied in practice. However, in 2018, the Polish Ministry of Justice published the draft Act on the Liability of Corporate Entities for Acts Prohibited under Penalty (the Draft Liability Act), the aim of which is to change the current framework for corporate criminal liability and make it more efficient. Work on the Draft Liability Act is still at the initial stage of the legislative process. The main assumptions of the proposed Draft Liability Act are as follows: (1) the liability of the corporate entity is to be independent of any previous conviction of an individual; (2) a corporate entity may be liable for any offence; and (3) a fine of up to 30 million złotys could be imposed on a corporate entity.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Jurisdiction between the law enforcement authorities (police, public prosecutors and criminal courts) depends on the subject matter and location of the offence. Higher branches of the public prosecution system have divisions devoted to corporate crimes where the prosecutors specialise in cases such as bribery and corruption, cybercrime or financial crime.

Aside from the police and public prosecutors, there are multiple specialist agencies with law enforcement powers, including:

- Internal Security Agency: the counter-intelligence agency, which focuses on issues concerning Poland's internal security, but also organised crime, corruption and economic coercion;
- Central Bureau of Investigation: the police agency that deals with organised crime;
- Central Anticorruption Bureau: tasked with investigating bribery and corruption; and
- Customs Service.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Criminal investigations may be initiated in cases where there is a justified suspicion that an offence has been committed. The relevant law enforcement agency may decide to do this on its own or based on the notification of a crime, which can be filed by anyone.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

According to the Polish Code of Criminal Procedure, notices or subpoenas must fulfil specific formal requirements and may be challenged if those requirements are not fulfilled. In the case of requests for documents and information, privilege or professional secrecy may be claimed.

© Law Business Research 2021

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Although currently Polish law does not provide for any leniency procedure in criminal cases, the approach of the corporate entity that is subject to a criminal investigation is taken into account. In relation to individual perpetrators, the Polish Criminal Code provides for a reduction of a penalty or exclusion of liability if the perpetrator discloses information concerning the crime to the authorities prior to its discovery.

The Draft Liability Act provides that the entity will be able to admit its liability voluntarily to avoid a trial and to agree a more lenient fine with the public prosecutor. Thus, if the draft Act enters into force, there will probably be an increase in the number of internal investigations carried out by companies wishing to benefit from the leniency procedure. Currently, work on the Draft Liability Act is not moving forward.

7 What are the top priorities for your country's law enforcement authorities?

Corruption, cybercrimes and financial crimes are currently high on the law enforcement authorities' agenda.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Although Polish law does not expressly provide for a compliance defence, it may be inferred from the current Liability Act. This is because such liability is dependent on fault: either fault in selection or organisational fault. In practice, having an effective compliance programme may enable the corporate entity to argue that organisational fault cannot be attributed to it. However, the use of this defence remains untested. In turn, if the Draft Liability Act enters into force, a corporate entity may be able to avoid criminal liability for corruption committed by the individuals and bodies authorised to act on its behalf if it proves that it acted with due care and diligence in the relevant circumstances. The corporate entity will have to prove that it had mechanisms in place to ensure compliance of its activities with the law. It can be expected that, for this purpose, the corporate entity will be able to rely on having a compliance programme.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

In Poland, cybersecurity is regulated by the Act on the National Cybersecurity System (the Cybersecurity Act) of 5 July 2018. It is the first law in Poland in this respect,

© Law Business Research 2021

implementing Directive (EU) 2016/1148 on security of network and information services (the NIS Directive) into the national legal system. The Cybersecurity Act came into force on 28 August 2018.

Apart from complying with all the requirements imposed by the NIS Directive (as described in the Europe Overview), the Polish legislator has extended the reach of the Cybersecurity Act by including the public administration and the telecommunications sector (to some extent) in its scope.

The Cybersecurity Act takes into account the regulations introduced by Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)).

Cybersecurity is also regulated to some extent by the amended Act on Payment Services (the Payment Services Act), which transposes the revised Directive (EU) 2015/2366 on payment services in the internal market into Polish law.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Polish Criminal Code covers various cybercrime offences, including, in particular, hacking, denial-of-service attacks, infection of information technology systems with malware, phishing, identity theft and identity fraud.

The law enforcement authorities frequently deal with cybercrimes, which have skyrocketed during the covid-19 pandemic. This often requires an international approach and multinational co-operation with authorities, both within and outside the European Union.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Polish criminal law has a general extraterritorial effect and applies to Polish citizens who commit criminal offences abroad (as long as the act in question is also a criminal offence in the country in which it was committed, and with any differences between the two legal systems used in favour of the accused). As regards criminal liability of corporate entities, the current law includes international entities that conduct business activity in Poland in the definition of corporate entities that may be subject to corporate criminal liability. This is largely untested and unclear. The aim of the draft Act on the Liability of Corporate Entities for Acts Prohibited under Penalty (the Draft Liability Act) is to clarify this situation and to specify that foreign corporate entities may be held liable for a criminal offence if it was committed in Poland, or if it was committed abroad but the consequences of the offence materialise in Poland, or if the act was against the interests of Poland or a Polish citizen or legal entity. At the same time, however, the Draft Liability Act stipulates that an investigation cannot be initiated against a foreign company, so it is unclear whether the Draft Liability Act would in fact facilitate penalising foreign corporate entities under Polish criminal law.

© Law Business Research 2021

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

One of the biggest challenges for the law enforcement agencies is how to effectively conduct large-scale cross-border investigations. Sometimes the lack of sufficient resources and proper forensic support makes it challenging to efficiently collect and analyse big volumes of seized data. Transnational corruption is another area in which the law enforcement agencies face challenges, as mutual assistance in criminal matters is often time-consuming.

The law enforcement agencies also encounter difficulties in gathering evidence. At present, the law does not create favourable conditions for companies to step forward and provide the authorities with documentation in exchange for leniency. Consequently, there are no sufficient grounds for co-operation (e.g., private investigations) aimed at developing better solutions for internal compliance.

In complex cybercrime investigations, the authorities are sometimes unable to identify the suspects (forming international crime groups) or to freeze stolen assets. This is because of lengthy, formal procedures that are not adapted to the developing schemes set up by cyber criminals. The situation is slightly better within the European Union, which has developed programmes for co-operation in cross-border investigations.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

There is neither an 'anti-piling on' nor a double jeopardy policy under Polish criminal law. The law makes it possible to investigate and punish the same criminal act that has been subject to a foreign criminal charge and sentence (for example, if a Polish entity that was part of a larger international conglomerate was penalised abroad for corruption, the relevant Polish law enforcement authority would aim to penalise the same entity in Poland, pursuant to Polish law). However, as regards individuals, any deprivation of liberty abroad will count towards any sentence issued in Poland.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common in Poland. Currently there are also no grounds for corporate settlements in criminal cases in Poland.

© Law Business Research 2021

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions made by foreign authorities may be taken into account by the Polish law enforcement authorities in terms of findings. However, these decisions are not binding on Polish investigations.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Poland does not have its own sanctions programme. Nevertheless, Poland is required to observe and enforce the United Nations Security Council sanctions and EU restrictive measures.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

We have not seen any landmark decisions relating to EU sanctions violations taken by the Polish courts or institutions. There are also no relevant cases relating to Council Regulation (EC) No. 2271/96 (the EU Blocking Regulation) and no specific blocking statue at the national level.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Polish authorities liaise with their counterparts in other countries for the purposes of enforcement.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The EU Blocking Regulation, which is applicable in Poland:

- prohibits all individuals living in the European Union and being citizens of one of the EU Member States, and all companies having their seat in the European Union, from complying with US acts imposing sanctions on Cuba, Iran and Libya;
- provides that no judgments or decisions giving effect to the above-mentioned US acts will be recognised or enforceable in EU Member States; and
- provides for a right to seek damages for harm caused as a result of application of the above-mentioned US acts.

© Law Business Research 2021

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Poland has not enacted any additional blocking legislation.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct most frequently come to light in companies as a result of reports by whistleblowers, internal investigations and private civil complaints (sometimes by competitors).

INFORMATION GATHERING

22 Does your country have a data protection regime?

Yes. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)) is directly applicable in Poland and regulates the vast majority of general data protection issues. Additionally, there is a Polish Data Protection Act of 10 May 2018, which regulates mostly administrative and procedural issues in respect of the Polish data protection authority (*Prezes Urzędu Ochrony Danych Osobowych*). Some specific issues in respect of data protection are also regulated in other legislative acts, such as the Labour Code or the Banking Law.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The data protection regime is enforced through mechanisms provided for in the GDPR (i.e., through inspections and the imposition of fines specified therein by the Polish data protection authority). The data protection authority uses the mechanisms provided for in the GDPR and has already imposed a number of fines for data protection breaches.

Apart from the above, breaches of data protection rules may sometimes constitute breaches of specific local acts and may lead to the imposition of sanctions provided therein. For example, sending marketing communications via electronic means or telephone without the explicit consent of the recipient is subject to fines specified in the Act on the Provision of Services via Electronic Means and in the Telecommunications Law, respectively.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Yes, the regulation of employee monitoring may cause concern in internal investigations.

© Law Business Research 2021

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Polish law regulates in detail the matter of employee monitoring. In principle, the monitoring of electronic communications of employees (and any other type of monitoring, apart from visual monitoring, which is based on slightly different criteria) may be introduced only if it is necessary to ensure the organisation of work that facilitates the full use of working time and the proper use of tools and equipment made available to employees. The scope, purposes and manner of monitoring should be agreed in a collective bargaining agreement, the work rules or (if the employer does not have a collective bargaining agreement and is not obliged to issue work rules) in a notification issued to employees. The employees must be notified about the introduction of monitoring no later than two weeks before it is put into operation.

The foregoing rules are mandatory, and the implementation of any monitoring that is not compliant with the rules is unlawful.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

The authorities quite often use search warrants or dawn raids to seize documents or data relevant to an investigation.

The authorities should act in line with the key principles that the seizure of data or documents must be (1) purposeful (i.e., it must serve the investigation's objectives), (2) necessary (it should be used as an *ultima ratio,* i.e., without the seizure, the investigation's objectives cannot be met), and (3) proportionate (i.e., the authorities are allowed to seize only the documents and data needed for the investigation, and nothing more).

If these limitations are exceeded, a company may file a complaint with the court, the purpose of which is to control the relevant authorities' actions. A company may also file civil claims against the State Treasury, if it proves that a seizure was unlawful and caused damage.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

A company cannot refuse to provide the authorities with privileged materials. However, if privileged material is subject to seizure, the company should adopt some additional measures aimed at its protection.

If the materials are subject to the attorney–client privilege, they should be provided in a sealed package or envelope. The public prosecutor is obliged to ask the court for permission to use such materials in an investigation. The court may grant permission (i.e., waive the privilege) as an *ultima ratio* (i.e., if the facts relevant to the investigation cannot be established without the use of the privileged materials).

© Law Business Research 2021

If the materials are protected by privilege that is attached to the defence counsel, they cannot be seized.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Witnesses have a duty to provide a testimony. However, there are significant exceptions from this rule:

- suspects may exercise their right against self-incrimination. They have the right to remain silent but not the right to lie (i.e., they may refuse to provide a self-incriminating testimony but may not mislead the authorities);
- witnesses may refuse to provide any testimony at all if they are related to the suspect (e.g., a spouse, an ascendant, a descendant, a sibling or a domestic partner);
- witnesses may refuse to answer specific questions, if the answer exposes them or a person related to them to any criminal liability; and
- witnesses who are legally obliged to keep relevant information confidential (for instance attorneys, because of their privilege) cannot disclose privileged information unless they are released from that obligation by a court.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

At present, Polish law does not include any provisions for whistleblower protection or incentives to whistleblowers.

Nevertheless, some regulations are expected to come into force soon, as Poland is obliged to implement Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (the EU Whistleblower Directive) by December 2021. The EU Directive obliges EU Member States to ensure the legal protection of reporting persons working in the private or public sector who (1) have acquired information about breaches of EU law in a work-related context, (2) have reasonable grounds to believe that the reported information is true and falls within the policy areas covered by the Directive and (3) reported the information internally, externally or by way of public disclosure. The legal protections are to include prohibition of any form of retaliation, access to support measures, ensuring the whistleblowers' right to an effective remedy and fair trial, as well as introducing penalties applicable to individuals that hinder or attempt to hinder reporting or retaliate. The EU Directive also requires EU Member States to ensure, at a minimum, that legal entities with 50 or more workers establish channels and procedures for internal reporting and follow-up of any whistleblower's report. Finally, it requires EU Member States to designate authorities competent to receive, give feedback and follow up on whistleblower reports and to provide these authorities with proper resources.

© Law Business Research 2021

On 18 October 2021, the Polish government published the first draft implementation bill. In general, the draft reiterates the provisions of the EU Directive. However, in some instances, the government has chosen to extend the scope of protection. For example, whistleblowers will be protected not only in the event of reporting breaches of specific acts of EU law, but also Polish law. Companies in the financial sector will be obliged to implement internal reporting channels regardless of how many employees they have.

There may be some challenges for certain large companies (i.e., those with more than 249 employees), which will have only two weeks (from the time the Polish implementation bill comes into force) to comply with the new law, in particular with respect to the requirements concerning internal reporting channels. Failure to comply may result in a fine and imprisonment.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There are no special legally protected rights for employees whose conduct is within the scope of an internal investigation. Employees are obliged to collaborate with the employer, but there are no specific laws requiring them to participate in an internal investigation (in the absence of any specific obligations set out in the employment contract). Employees should be informed that the investigation is conducted not in their personal interest but in the interests of the company. The employee must be protected at all times by the applicable data protection and privacy laws. There is no distinction between officers and directors of the company for that purpose.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

The law does not provide for any particular steps in this regard. However, the Polish Labour Code allows an employer to terminate the contract if an employee has engaged in misconduct.

Polish law does not entitle an employer to suspend an employee or the employee's right to receive compensation. The only situation in which it is possible to unilaterally release an employee from the duty to perform work (while retaining full right to remuneration) is during the notice period. The case law of Polish courts confirms that a suspension in any other situation (even while retaining the full right to remuneration) is unlawful. Nevertheless, the usual practice is that employees are suspended from performing their duties if it is necessary from the point of view of an investigation and if the good of the investigation overrides any employment risks.

© Law Business Research 2021

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Generally, the employees to whom the Polish Labour Code applies are obliged to collaborate with their employer, but there are no legal consequences, for example, for declining to participate in a witness interview. Depending on the specific set of circumstances, including the obligations included in the employment contract, an employee may be dismissed for refusing to collaborate with his or her employer.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Although the conduct of internal investigations is not regulated, it is practical to set out the scope of the investigation at its outset. That scope would be included later in the investigation report, so it is clear which issues have been investigated by the company. This would cover the allegations of irregularities and facts to be verified, the list of employees to be interviewed and the categories of documents to be collected, and include an outline of the action plan for the investigation.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

In such a case, the company should prepare for the opening of a criminal investigation by the authorities. Although there is no obligation to do so, it is advisable for the company to conduct an internal investigation. The internal reporting obligations will depend on the company's policies.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

In these circumstances, the company would be obliged to produce the documents (unless it is entitled to object, for example, based on privilege) and, therefore, should take all necessary steps to enable the preservation and production of the documents. Those steps may include sending out a document preservation notice (although it must first be decided whether sending out such a notice would risk the documents being destroyed or concealed) or identifying relevant search terms and custodians.

© Law Business Research 2021

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Under Polish law, there is no obligation to self-report in relation to corporate crimes or an internal investigation. The decision to disclose depends on the interests of the company. If the company decides to self-report, it is advisable to disclose the information only after the internal investigation has been fully completed.

There is an exception concerning banks (which under Polish law must inform the authorities without undue delay of any justifiable suspicion that the bank's activity is being used to conceal a tax crime, to finance terrorist activities or to launder money) and financial institutions (which are obliged to report suspicious financial transactions to the relevant financial authorities).

37 How are internal investigations viewed by local enforcement bodies in your country?

So far, Polish law has not provided for any guaranteed benefits from conducting an internal investigation. However, it might be taken into account when the law enforcement authorities or the courts are considering the appropriate penalty for the corporate entity or related individuals. An internal investigation is also considered useful by the authorities, who are willing to use the findings of the investigation for their own purposes.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Yes. A company may claim the attorney–client privilege, for example, over investigation reports or protocols. The privilege applies if these documents are prepared by an attorney.

However, a company may be obliged to provide such documents to the authorities in other circumstances, in particular if requested and the facts relevant to the investigation cannot be established without the use of the privileged materials.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The attorney–client privilege in Poland originates from a lawyer's duty to keep all the affairs of a client confidential. This is legally protected by the right to remain silent if examined as a witness. It also covers documents providing legal advice, as well as communications between lawyers and their clients concerning legal advice.

As a rule, an attorney is the holder of privilege. However, it follows from case law that because the purpose of the privilege is to protect the client's interests, the client may

© Law Business Research 2021

also claim that certain information or documents are privileged and, therefore, cannot be disclosed to the authorities.

The same rules apply to both corporations and individuals.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Generally, the attorney–client privilege applies equally to in-house and external counsel. Polish regulations provide for specific guarantees of independence of the in-house counsel (i.e., they should have an independent position in a company and report directly to the headquarters).

However, since Poland is an EU Member State, specific requirements regarding in-house counsel provided for in the case law of the Court of Justice of the European Union also apply (for instance, as described in the *Akzo Nobel* case). Therefore, the application of privilege to in-house counsel may be challenged, in particular in antitrust investigations carried out by the European Commission.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Polish law distinguishes between EU lawyers and non-EU lawyers. EU lawyers (listed by the bar of advocates or the bar of legal advisers) have the same scope of powers and duties as Polish lawyers. Non-EU lawyers, on the other hand, may provide legal advice and prepare legal opinions regarding the law of the country of their qualification or international law.

Therefore, the attorney–client privilege in relation to advice concerning investigations in Poland applies equally but only to Polish and EU lawyers.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Polish law does not provide for a general concept of a waiver of the attorney–client privilege.

However, the client (not the attorney, who has a duty of confidentiality) may decide to disclose the information protected by the attorney–client privilege to the authorities. It may be regarded as a collaborative step in certain circumstances, although there are no specific provisions of law addressing this issue.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Polish law does not provide for a general concept of limited waiver of the attorney–client privilege. However, if a company produces privileged information to law enforcement of its own volition), it does not mean that it has to provide the information to other third parties.

Third parties, however, may request the public prosecutor to provide privileged information that is collected in the course of a criminal investigation, if specific criteria are

© Law Business Research 2021

met (i.e., disclosure does not undermine the correct conduct of the investigation or an important state interest). An interest of the party who shared privileged information is not a factor that the public prosecutor has to take into account.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Waiver of privilege in another country has no direct legal effect on claiming privilege in Poland.

However, it cannot be entirely ruled out that the authorities may seize privileged documents or information from a third party in another country if that party cannot claim privilege under Polish law.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Polish law does not provide for a general concept of common interest privilege. However, privilege in Poland is also linked to specific information or documents and not only to a person who is the recipient of privileged information or documents. Therefore, if the privileged information is voluntarily shared with a third party, then the third party may also claim that the information is privileged.

In any event, the third party may be obliged to provide privileged information or documents to the authorities in certain circumstances, in particular if requested and the facts relevant to the investigation cannot be established without the use of the privileged materials.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

The attorney–client privilege in Poland originates from a lawyer's duty to keep all the affairs of a client confidential. A lawyer has a duty to keep confidential all the information received in relation to the provision of legal services.

Therefore, if a lawyer benefits from the assistance of third parties (e.g., external experts or consultants), he or she may claim that the information or documents produced by the third party were provided in relation to the provision of legal services.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no regulations permitting or prohibiting witness interviews and, therefore, they are conducted informally. The provisions of the Code of Criminal Procedure concerning witness testimonies (and, in particular, a witness's right to refuse to answer certain questions) do not apply to such interviews, although statements made by witnesses may affect the criminal proceedings.

© Law Business Research 2021

However, participation in an interview is based on an employee's duty to collaborate with the employer or on specific contractual obligations towards the employer, and is voluntary in this respect. The employees generally do not face any legal consequences for refusing to be interviewed, apart from those stemming from the company's policies. Similarly, third-party employees or former employees cannot be coerced into attending the interview.

If the witness is an employee within the meaning of the Polish Labour Code, he or she generally has an obligation to maintain the confidentiality of company secrets or information that could cause harm to the employer.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes, a company may claim the attorney–client privilege if any such interview protocols or reports have been prepared by an attorney.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

As the manner of conducting internal investigations is not regulated under Polish law, there are no specific requirements for warnings or information to be provided to the witnesses interviewed in the course of an internal investigation.

However, in practice, *Upjohn* warnings explaining that the interviewing attorney acts on behalf of the company and not the interviewee are used, especially in cases where the company in question may be subject to US anti-corruption laws.

Regardless of the foregoing, the personal rights of the interviewee and the data protection laws should always be taken into account by the interviewing team. Also, if the employee is a member of a trade union within the meaning of the Polish Labour Code, a trade union representative may have to be present during the interview.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There are no specific regulations as to the conduct of a witness interview. However, the interview would typically be conducted by an attorney who is a member of the internal investigation team. At the outset, the attorney will give an *Upjohn* warning, explain the purpose of the interview and ask the interviewee to keep the meeting confidential. The attorney will take notes from the meeting. Notes from interviews may be used as evidence in criminal proceedings, for instance to verify testimonies before the courts.

Documents may be shown to a witness during an interview but are usually not provided to the witness before the meeting.

Owing to the informal nature of witness interviews conducted as part of an internal investigation, if an interviewee asks for his or her legal representative to be present, there are no grounds to force the witness to attend the meeting without such representation.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Generally, under Polish law there is no legal obligation to report misconduct to law enforcement authorities (i.e., to self-incriminate).

However, Polish law provides for specific rules under which an individual or an entity, having knowledge about the misconduct of others, is obliged to report it to law enforcement authorities. The Polish Criminal Code provides that failure to notify the law enforcement authorities about specific criminal offences (against the state, life and health, personal freedom or of a terrorist nature) is a criminal offence in itself.

On a related note, the provisions of law concerning cybersecurity issues, data protection, money laundering or taxes also include obligations to report certain incidents or transactions that are not necessarily misconduct per se.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

It depends on the facts and circumstances of an individual case. The bottom line is that self-reporting may be advisable (e.g., in corruption-related matters) if a company (or those of its directors or officers who may be held individually liable for a criminal offence) may gain any kind of advantage in this way.

Under the Polish Criminal Code, an individual cannot be held liable for offering or giving a bribe to a public official (or to a manager in the case of managerial corruption), if he or she discloses all material facts of the criminal offence to the relevant law enforcement authority before the authority discovers the offence on its own.

Another example relates to the criminal offence of abuse of trust, or acting to the detriment of the company. If an offender voluntarily redresses the damage caused to the company by such an offence before the criminal investigation is initiated, he or she cannot be held liable for the offence.

Similarly, an individual cannot be held liable for a criminal tax offence (or a tax misdemeanour) if, after the offence was committed, he or she (1) notified the law enforcement authority about all material facts relating to the offence, in particular about the other offenders taking part in a criminal scheme, (2) paid the entire tax debt and (3) cannot be considered a person organising or ordering a criminal tax offence, inducing others to do so or leading a group of offenders.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The timing is crucial. Self-reporting may be advantageous for an individual or a company if it is made either before the law enforcement authorities learn about a criminal offence on their own, or before a criminal investigation is initiated. Therefore, the company should

© Law Business Research 2021

try to verify whether this is the case in a particular matter (although it may be very difficult in practice because of the principle of secrecy of the criminal investigation).

Before any irregularity is self-reported, a company should also establish all material facts thereof, in particular by way of an internal investigation and assessment of all related legal, operational and public relations risks.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Yes, it is quite common in practice. Law enforcement authorities usually list the information, documents, data, hardware, etc. they require in a subpoena. If there are any doubts as to the scope of materials to be provided, it is always worth seeking clarification from the authorities.

A company should not obstruct an investigation. It should co-operate with the law enforcement authority but should not be overly accommodating.

Although there are no procedural rules to do this, a company may also address the authority's potential concerns even before the charges are brought. For example, it is sometimes worth providing written explanations to the authority if the company learns about any allegations filed with the authority by a third party.

After the charges are brought, an individual or the company may provide their explanations. This can be done at any stage of the proceedings.

55 Are ongoing authority investigations subject to challenge before the courts?

The decision to start an investigation or to bring charges against an individual or a company cannot be challenged before the courts. However, a party to the investigation (the suspect or the aggrieved party) may file a complaint with the court if the investigation is prolonged, and may seek liquidated damages of up to 20,000 złotys.

The decision to refuse to commence or to discontinue an investigation may be challenged by an aggrieved party, or a party that cannot be considered aggrieved but has notified the authorities about a criminal offence that violated its rights.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

There are no provisions of Polish law addressing this issue. Fundamentally, the scope of the subpoena issued by the authorities is non-negotiable and the party requested to provide materials has a duty to do so. Of course, a party requested to provide materials may contact the authorities to request clarification of any potential doubts.

© Law Business Research 2021

In practice, subpoenas issued by foreign authorities should be enforced in Poland by the Polish authorities. The Polish Code of Criminal Procedure provides for the rules governing international legal aid in the course of the pending investigation as follows:

- If the authorities from an EU Member State request enforcement of a subpoena, the Polish authorities may refuse to enforce it only if (1) the act in relation to which the subpoena has been issued is not a criminal offence under Polish law (with some exceptions), (2) the evidence listed in the subpoena cannot be collected (e.g., because it has been lost or damaged or cannot be found), (3) the subpoena relates to a criminal offence in respect of which the criminal investigation has ended with a final and binding judgment, or (4) other formal requirements (concerning mainly related documentation) are not met.
- If the authorities from non-EU states request enforcement of a subpoena, the Polish authorities may refuse to enforce the subpoena if its enforcement is contrary to the fundamental principles of the Polish legal system or if it violates the sovereignty of the Republic of Poland.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

No. Companies are not obliged to produce materials from abroad. In practice, companies often explain in their responses to subpoenas that they are not in possession of, or do not have access to, materials located abroad and another entity may have to respond.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Yes. Within the European Union, this is regulated mainly by the Treaty on the Functioning of the European Union (Articles 82 to 89), regulations concerning Europol, Eurojust and specific regulations and directives focused on particular types of criminal offences or procedural issues. However, Poland has not accessed the European Public Prosecutor's Office, which has been operational since 1 June 2021.

The respective EU regulations are implemented into Polish law and refer mainly to (1) the collection of evidence and confiscation of freezing measures, (2) conducting investigative actions (e.g., on the basis of an European Investigation Order), (3) enforcement of a European Arrest Warrant, or (4) implementation of other precautionary measures.

In the case of non-EU states, the Polish authorities have a general duty to co-operate. However, they may refuse to provide legal assistance if:

- to do so would be contrary to the fundamental principles of the Polish legal system;
- it violates the sovereignty of the Republic of Poland;
- a request for legal assistance comes from a country that does not provide reciprocity;

© Law Business Research 2021

- a request is made in relation to an act that cannot be considered a criminal offence under Polish law; or
- the requested legal assistance is outside the scope of powers granted to the public prosecutor's office in Poland.

The Polish authorities may also form investigative teams with the authorities from other countries.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

There is a general rule of secrecy of a criminal investigation. Public disclosure of information about a criminal investigation is a criminal offence in Poland.

However, the public prosecutor may – at his or her sole discretion – decide about public disclosure of information about a particular investigation (also in the media). The Polish law on the Public Prosecutor's Office enables the General Prosecutor, the Deputy General Prosecutor and the public prosecutors authorised by them to share information concerning particular investigations with third parties if sharing that information may be significant for national security and the proper functioning of the state.

Third parties' access to investigation files is also determined by the public prosecutor at his or her discretion. The public prosecutor may refuse to grant access to the files only if access would undermine the correct conduct of the investigation or an important state interest.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

We would advise a company to respond to the law enforcement authority that it is unable to provide documents from another country because of local laws, and to suggest that the authority should use the formal procedure for co-operation with the local enforcement authority.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Council Regulation (EC) No. 2271/96 (the EU Blocking Regulation), which is applicable in Poland:

- prohibits any individuals who live in the European Union or who are citizens of any EU Member State, as well as companies having their seat in the European Union, from complying with any US acts imposing sanctions on Cuba, Iran and Libya;
- provides that no judgments or decisions giving effect to the above-mentioned US acts will be recognised or enforceable in EU Member States; and

© Law Business Research 2021

- provides for a right to seek compensation for any damage sustained as a result of the application of the above-mentioned US acts.

Therefore, if a subpoena is based on or concerns one of the US acts listed in the EU Blocking Regulation, the party receiving the subpoena should not respond to it, unless it is granted special permission by the European Commission.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production may not be advisable if it does not give any advantage to the company in a particular case. It may expose the company, for example, to a risk that the law enforcement authorities would incorrectly consider specific actions of the company unlawful and would like to 'dig deeper'. If the company wishes to disclose information voluntarily, the data protection issues should also be considered.

Compelled production, on the other hand, may be adapted to the actual needs of the law enforcement authority. In such cases, the company must not produce any documents that are not necessary for the law enforcement authority. In terms of data protection regulations, in such cases the company has a clear legal basis to produce materials.

The materials provided to the law enforcement authorities may be discoverable by third parties, in particular if they prove that their access would not undermine the correct conduct of the investigation or an important state interest. The public prosecutor may – at his or her sole discretion – decide about public disclosure of information about a particular investigation (including in the media) if sharing that information may be significant for national security and the proper functioning of the state.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Individuals can be liable to fines, restriction of liberty (in the form of community service or salary deduction) or imprisonment. There are also some additional punitive measures that may be adopted, namely (1) a ban on holding specific functions, practising specific professions or pursuing business activities of a specific kind, (2) publication of the judgment, or (3) an obligation to redress any damage resulting from a criminal offence.

Currently, companies can be liable to fines of up to 5 million złotys, but not more than 3 per cent of the revenues generated in the financial year in which the prohibited act was committed. Additional punitive measures that may be imposed on a company are as follows:

- forfeiture of assets or economic gains originating from, or used to commit, the prohibited act;
- prohibition of promotions or advertising;
- prohibition of the use of financial support from public funds;

© Law Business Research 2021

- prohibition of seeking the award of public contracts; or
- publication of the judgment.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

If a company wants to settle in another country, there is a risk that the settlement will be used to its disadvantage in Poland (as the evidence that a criminal offence or prohibited act being subject to the settlement was actually committed). Therefore, if this is the case, the company should assess the risk of liability in Poland and, in particular, the chances of a successful defence against that liability, based inter alia on the compliance defence or rules providing for the exclusion of double jeopardy.

65 What do the authorities in your country take into account when fixing penalties?

The criteria for fixing penalties for individuals are provided for in the Polish Criminal Code and include:

- the degree of guilt;
- the degree of public harm and any other negative consequences caused by a criminal offence;
- the preventive and educational objectives that the penalty is to achieve;
- the need to develop legal awareness in society;
- the types of duties breached; and
- the efforts to redress the damage.

In terms of companies, the criteria include:

- the scope of irregularities in choosing or supervising individuals who are personally liable for a criminal offence;
- the scope of economic gains originating from the criminal offence;
- the financial situation of the company; and
- the impact of the penalty on the future operation of the company.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Neither non-prosecution agreements nor deferred prosecution agreements are available for corporations in criminal cases in Poland.

The 2018 draft Act on the Liability of Corporate Entities for Acts Prohibited under Penalty (the Draft Liability Act) provides for a settlement-like tool in dealings with the public prosecutor, allowing corporate entities to avoid widespread legal consequences of a criminal offence. In particular, the public prosecutor will be able to file a motion for a voluntary submission of a corporate entity to criminal liability to be approved by the court if the following prerequisites are met: (1) the circumstances of the criminal offence

© Law Business Research 2021

are beyond doubt; (2) the corporate entity has disclosed to the authorities information about the criminal conduct of an individual committing the offence; and (3) the corporate entity has paid the equivalent of the damage caused by the offence and the equivalent of the lowest financial penalty for the offence, and has consented to forfeiture. The final judgment will not be recorded in the criminal register.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There are currently no regulations on reporting restrictions or anonymity since it is not possible for corporations to enter into non-prosecution agreements or deferred prosecution agreements in criminal cases in Poland.

The Draft Liability Act does not provide for any related regulations.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Under the Draft Liability Act, the public prosecutor will be able to file a motion for a voluntary submission of a corporate entity to criminal liability to be approved by the court if the following prerequisites are met: (1) the circumstances of the criminal offence are beyond doubt; (2) the corporate entity has disclosed to the authorities information about the criminal conduct of an individual committing the offence; and (3) the corporate entity has paid the equivalent of the damage caused by the offence, and the equivalent of the lowest financial penalty for the offence, and has consented to forfeiture.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Polish law currently does not provide for the use of external corporate compliance monitors by Polish law enforcement authorities.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Civil proceedings might take place in parallel with criminal matters. Private plaintiffs might gain access to criminal files.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

There is a general rule of secrecy of the criminal investigation but the prosecutor may decide to disclose information about the investigation publicly.

© Law Business Research 2021

If a case is being heard before a court, it essentially becomes public (with some exceptions for specific procedures). Also, the media may broadcast the trial. The court may, however, exclude the public from a trial if (1) the circumstances discussed should be kept confidential because of a significant state interest, or (2) there is a need to protect an important private interest. In any event, the judgment is announced publicly.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Yes. In such cases, close co-operation between legal and public relations advisers is advisable, so that the corporate communication is aligned with the corporate legal defence strategy.

73 How is publicity managed when there are ongoing related proceedings?

Because of the general rule of secrecy of the criminal investigation, the charges brought by the law enforcement authorities cannot be commented on publicly. However, this rule does not apply when a case is brought before a court or in the case of civil proceedings.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Generally no, but it may be required with respect to publicly listed companies.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

EU laws on ESG reporting apply in Poland. For example, following the EU requirements, the Polish law on accounting has recently introduced a provision that requires the biggest financial institutions and publicly traded companies (e.g., with 500 employees or more or 85 million złotys of total balance sheet assets per annum) to report in their financial statements non-financial issues, including ESG risks, policies etc. in a manner allowing the company's effects on the environment and social aspects to be assessed. The Polish stock exchange has also recently published guidelines on ESG reporting for publicly traded companies.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Yes, we expect to see the implementation of further EU laws on ESG reporting, including the EU Green Deal laws, such as Regulation (EU) 2020/852 on the establishment of a framework to facilitate sustainable investment (the EU Taxonomy Regulation), which will enter into force in January 2022, or the planned Corporate Sustainability Reporting Directive.

© Law Business Research 2021

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Yes, ESG-related litigation is an increasing trend in Poland.

Recently, an environmental non-governmental organisation, Client Earth, has initiated two litigations against state-related energy conglomerates in relation to the coal-fired power plants operated by them.

In a case against Enea SA, Client Earth sought an annulment of Enea's management board resolution giving consent to the construction of the Ostroleka C power plant. The case was decided in favour of Client Earth.

In a case against PGE SA, Client Earth demanded that PGE reduce the greenhouse gas emissions from Europe's largest power plant, Belchatow, which is operated by PGE. The first instance court ruled that PGE must negotiate and settle the effects of Belchatow on the climate, although no settlement was reached by the prescribed deadline.

Client Earth is also representing five Polish citizens who have recently sued the Polish State Treasury in the Polish courts for inaction on the climate crisis, demanding the state's admission of responsibility to adhere to the Paris Agreement (the international treaty on climate change) and redress the emission of greenhouse gases. All five cases are being heard by different district courts in Poland.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Although the amendment of the corporate criminal liability law is a long-awaited legislative change, the implementation of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (the EU Whistleblower Directive) is expected to be the key legislative change to be made in the compliance field.

© Law Business Research 2021

20

Russia

Hannes Lubitzsch[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

In 2021, some of the highest-profile corporate investigations being conducted by the Federal Antimonopoly Service (FAS) and the Russian data protection authority, Roskomnadzor, are against Western technology companies.

For example, in August 2021, FAS imposed a fine of 1.3 billion roubles on Booking.com (11.5 per cent of its annual turnover in Russia in 2020) for abusing its dominant market position. In April 2021, FAS opened an investigation against Google for abusing the dominant market position of YouTube. In October 2021, another investigation was opened against Apple for prohibiting Russian developers from informing buyers of applications in the App Store of alternative payment methods.

In March 2021, Roskomnadzor slowed down Twitter for not removing forbidden content. In August 2021, a Russian state court confirmed the fines imposed by Roskomnadzor on WhatsApp (4 million roubles), Facebook (15 million roubles) and Twitter (17 million roubles) for violating the Russian data localisation requirements. In August 2021, Roskomnadzor ordered Apple and Google to remove from their stores all applications used to further extremist activities.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held liable only for violations of the Administrative Offences Code. Individuals can be held liable for violations of the Administrative Offences Code and the

1 Hannes Lubitzsch is an associated partner at Noerr.

© Law Business Research 2021

Criminal Code. Under Russian corporate law, each director of a company (supervisory board member, general director and member of the management board) can be held liable by the company's shareholders for damage caused to the company as a result of culpable actions or omissions. In practice, directors are regularly held liable for damage caused to their companies by the payment of fines under the Administrative Offences Code.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Offences under the Administrative Offences Code (committed by corporations and individuals) are investigated by the Public Prosecutor's Office or by other law enforcement authorities that perform supervisory functions in certain areas, such as the FAS and Roskomnadzor.

Offences under the Criminal Code (committed by individuals) are generally investigated by the Public Prosecutor's Office. The relevant functions of the Public Prosecutor's Office are distributed among (1) the General Prosecutor's Office at the federal level, (2) the prosecutor's offices in the 85 'subjects of the Russian Federation' at the regional level, and (3) the prosecutor's offices of the districts and cities at the municipal level.

In addition, the Investigative Committee of the Russian Federation – a federal authority previously part of the of the Public Prosecutor's Office but now (since 2011) separate and subordinated directly to the President of the Russian Federation – performs pre-investigative reviews of notifications on offences and preliminary investigations against individuals for certain offences under the Criminal Code. The Investigative Committee performs its functions at the federal, regional and municipal levels, through (1) its central office at the federal level, (2) investigative departments in the subjects of the Russian Federation, and (3) investigative departments of the districts and cities.

In some cases, the prosecuting functions of several law enforcement authorities may overlap. For example, violations of antitrust requirements during public procurement processes – especially state tenders (which are investigated by the FAS) – are often accompanied by bribery and corruption offences. Following the completion by FAS of its own investigation and the imposition of administrative penalties for the violation of antitrust requirements, the matter may then be transferred to the Public Prosecutor's Office for the opening of bribery investigations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

An administrative case (against corporations and individuals) can be opened by the competent law enforcement authority based on (1) the direct discovery of facts that sufficiently indicate that an administrative offence has been committed, (2) materials received from other law enforcement authorities and non-government organisations, which contain facts indicating the commission of an administrative offence, and (3) reports from individuals and legal entities, or mass media information, that contain such facts. An administrative investigation is initiated with the opening of the case if time-consuming procedural actions must be taken to clarify all circumstances of the offence.

© Law Business Research 2021

A criminal case (against individuals) can be opened based on (1) the reporting of a criminal offence by individuals or public officials, (2) voluntary self-reporting by the criminal offender and (3) information about a criminal offence received from other sources. In each case, facts are required that sufficiently indicate the existence of the elements of a criminal offence.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

As a general rule, a notice or subpoena from a law enforcement authority, which violate the rights or legal interests of the company and do not comply with Russian legislation, can be challenged in a Russian state court. The procedure for challenging a notice or subpoena depends on the legal basis of the relevant act.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

There is no option to enter into co-operative agreements for suspects in administrative proceedings (corporations and individuals) under the Administrative Offences Code.

Since 2009, the Criminal Procedural Code allows 'pretrial co-operation agreements' with suspects in criminal investigations (but individuals only), including for bribery and corruption offences. They are particularly relevant for individuals who have committed offences about which they cannot self-report to be excluded from liability, as defined in Article 290 of the Criminal Code (bribe-taking by a public official). Under a pretrial co-operation agreement, the defendant undertakes to assist in the investigation of other individuals who participated in the relevant offence. If all statutory requirements are met, the defendant's sentence will be reduced to not more than half the maximum punishment for the relevant offence under the Criminal Code.

7 What are the top priorities for your country's law enforcement authorities?

According to statistics published by the Russian Ministry of the Interior for 2020, Russian enforcement actions against white-collar crime focused on cybercrime (roughly 25 per cent of all registered criminal offences), fraud (16 per cent), economic crime (5 per cent) and bribery and corruption (1.5 per cent).

Anti-bribery and corruption enforcement actions against corporations focus on bribery of domestic public officials. According to statistics published by the Russian Supreme Court for 2020, a total of 322 corporations were convicted of all types of bribery (as defined in Article 19.28 of the Administrative Offences Code, i.e., unlawful remuneration on behalf of a legal entity). As in the past, most corporations were fined for bribing domestic public officials, a category that also includes employees of the many state-owned companies that are characteristic of the Russian economy.

Bribing public officials also involves the greatest liability risks for individuals. In 2020, there were 4,446 convictions for bribery of public officials (giving or taking a bribe

© Law Business Research 2021

as defined in Articles 290, 291 and 291.2 of the Criminal Code) compared with only 201 convictions for commercial bribery (as defined in Article 204 of the Criminal Code).

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Under the Administrative Offences Code, a corporation will be guilty of an administrative offence if it can be established that it did not take all necessary measures to ensure compliance with the violated regulations and this violation constitutes the relevant administrative offence. That means that a corporation accused of an administrative offence, as defined in Article 19.28 of the Administrative Offences Code (unlawful remuneration on behalf of a legal entity), may claim that it has taken all measures necessary to prevent bribery by its employees or agents.

In particular, the legal entity may arguably claim that it fully complied with its obligations under Article 13.3 of the Anti-Corruption Law to take anti-corruption measures to be exempt from administrative liability. These measures include those that must be taken by Russian organisations according to Article 13.3 of the Anti-Corruption Law (appointment of a compliance officer, adoption of a compliance code, prevention of conflicts of interest, co-operation with law enforcement authorities, etc.). The Russian Labour Ministry has issued detailed recommendations for their implementation.

Since 2018, the Supreme Court of the Russian Federation has expressly referred to the requirements of Article 13.3 of the Anti-Corruption Law when reviewing cases of corporate bribery. Some of the lower courts have also referred to Article 13.3 in their decisions. Further, the prosecutor's offices at the municipal level apparently have started to consider non-compliance with these requirements when bringing bribery charges against legal entities. However, the authorities and courts failed to answer the decisive question: to what extent the implementation of these measures may exempt companies from liability, or reduce their liability, in a specific administrative case.

In the prosecution of Russian Standard Bank for corporate bribery in 2019–2020, case law on the benefits of a compliance management system was developed further. For the first time, a higher Russian court (i.e., the Fourth General Jurisdiction Court of Cassation) elaborated on the specific anti-corruption measures that a company must take to be excluded from liability for bribery. Although the relevant decision was subsequently vacated on procedural grounds, it provided an interesting insight into the requirements that courts may place on compliance management systems. In this particular case, the court was of the opinion that all necessary measures to prevent the offence had been implemented because the bank had adopted an internal anti-corruption regulation, familiarised the relevant employees with this regulation, and incorporated a general obligation to comply with these internal regulations into the employment agreement. This means that, in certain circumstances, even taking a few formal anti-corruption measures may suffice to shield a company from liability for bribery.

Following legislative changes that entered into force in March 2020, corporations may adopt an antitrust compliance programme consisting of certain measures that are

© Law Business Research 2021

listed in the law. This compliance programme must be adopted in the form of an internal document at company or group level, which is then published on the internet. A properly adopted compliance programme may reduce or even exclude liability for antitrust violations under the Administrative Offences Code.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Cybersecurity is regulated mainly by Federal Law 187-FZ 'On security of critical information infrastructure . . .' which entered into force on 1 January 2018. This Law imposes certain obligations on authorities, organisations and companies that operate information systems, telecommunication networks or automated control systems in sectors that are strategically important for the state – healthcare, science, transport, communications, power, financial markets, fuel and energy, defence, space rockets, mining, metallurgical and chemical industry. Their obligations include a categorisation of the relevant critical information infrastructure and taking measures to protect the entity against cyberattacks depending on the results of that categorisation. Compliance with the law is monitored by the Federal Service for Technical and Export Control.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Chapter 28 of the Criminal Code prohibits various forms of cybercrime, including cyberattacks (unlawful interference with critical information infrastructure: Article 274.1) and hacking (unlawful access to computer information: Article 272).

Countering cyberattacks on information systems, telecommunications networks and automated control systems falls into the competence of the Federal Security Service (the FSB). Various acts of computer fraud and phishing are investigated by the Russian police and other law enforcement authorities who have created separate divisions specifically for the purpose of fighting cybercrime.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Only certain provisions of Russian administrative and criminal law have extraterritorial effect. In particular, Article 19.28 of the Administrative Offences Code (unlawful remuneration on behalf of a legal entity) prohibits the bribery of foreign public officials by corporations. This offence punishes the illegal transfer, offering or promise of money, securities or other property, valuable services or other property rights to a foreign public official on behalf, or in the interest, of a corporation, in return for the foreign public official using his or her authority to act in favour of the corporation. A foreign public

© Law Business Research 2021

official is defined as any appointed or elected person holding any position in a legislative, executive, administrative or judicial body of a foreign state, and any person performing any public duties for a foreign state, including for a public authority or public enterprise.

Since March 2016, Russian law enforcement authorities may prosecute domestic and foreign corporations for bribery offences committed outside Russia. Prosecution in this context requires additional justification: the offence must be directed against the interests of the Russian Federation or that possibility must be established by international agreements acceded to by the Russian Federation (Administrative Offences Code, Articles 1.8(3) and 2.6(2.1)). Since the term 'interests of the Russian Federation' is not defined under Russian law, theoretically any foreign bribery offence involving a Russian element may be subject to administrative proceedings in Russia.

The bribery of foreign public officials by individuals is prohibited by Article 291 of the Criminal Code (giving bribes). According to the applicable court practice, this offence punishes the payment of bribes in return for (1) a foreign public official using his or her authority to act in favour of the bribe giver or the persons represented by him or her, (2) the foreign public official enabling another public official to take such actions, (3) general patronage or (4) general connivance. Further, Article 291.1 of the Criminal Code (mediation in bribery) punishes individuals for the direct transfer of bribes to foreign public officials on a considerable scale (i.e., exceeding 25,000 roubles) on instructions by the bribe giver or bribe taker, as well as promises and proposals of such transfers. Smaller bribery offences committed by individuals (those involving bribe payments to foreign public officials not exceeding 10,000 roubles) are punishable under Article 291.2 of the Criminal Code (small-scale bribery).

Russian citizens can be held liable for any offence under the Criminal Code that has been committed outside Russia (Criminal Code, Article 12(1.)). Foreign citizens can be prosecuted for criminal offences if they are directed against the interests of the Russian Federation or that possibility is established by international agreements (Criminal Code, Article 12(3.)).

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Up to now, Russian anti-bribery enforcement actions have been limited almost entirely to purely domestic cases. Foreign individuals who are not from a Member State of the Commonwealth of Independent States are punished only sporadically; foreign corporations are prosecuted only in exceptional cases. Despite Russia's accession to the Organisation for Economic Co-operation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions in 2012, there seems to be no prosecution of bribery of foreign public officials.

Cross-border investigations by foreign law enforcement authorities or multinational companies regularly require the transfer of protected data from Russia to foreign jurisdictions. The collection and cross-border transfer of such data is subject to extensive Russian regulation. In particular, the transfer of the personal data of Russian citizens requires the relevant individuals' written consent to the transfer. Since the consent can be difficult to obtain in practice, the relevant data may have to be depersonalised before the transfer.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

In certain circumstances, Russian law enforcement authorities may prosecute domestic and foreign corporations for offences under Article 19.28 of the Administrative Offences Code (unlawful remuneration on behalf of a legal entity) committed outside Russia. However, the law expressly prohibits double jeopardy – Russian jurisdiction arises only if the corporation has not been held liable in a foreign state.

Foreign citizens must not be prosecuted in Russia for a criminal offence committed outside Russia if they have been convicted for this offence in a foreign state.

There is nothing analogous in Russia to the 'anti-piling on' policy as exists in the United States to prevent multiple authorities seeking to penalise companies for the same conduct.

14 Are 'global' settlements common in your country? What are the practical considerations?

Not applicable.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

To date, none of the foreign enforcement actions based on bribery and corruption offences relating to Russia (in particular under the US Foreign Corrupt Practices Act or the UK Bribery Act) seem to have triggered any subsequent investigations by Russian law enforcement authorities.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Russia's sanctions programme consists mainly of economic sanctions and measures that have been introduced to respond to the sanctions imposed on Russia by the United States and the European Union.

On 7 August 2014, an import ban on agricultural products, raw materials and food from the United States, EU Member States and other states supporting the anti-Russia sanctions was initially imposed for one year and has been regularly extended since then. This import ban is based on Federal Law 281-FZ 'On special economic measures' of 30 December 2006, which authorises the Russian president to take temporary measures to respond to unfriendly actions by foreign states that threaten the interests of the Russian Federation.

© Law Business Research 2021

Federal Law 127-FZ 'On measures (countermeasures) in response to unfriendly actions of the United States . . .' came into force on 4 June 2018. This Law constitutes another basis for the Russian president to take extensive economic countermeasures against the United States and other 'unfriendly states' supporting the anti-Russia sanctions. In contrast to measures under Federal Law 281-FZ, countermeasures under this law can be unlimited in time. The taking of any countermeasures is at the sole discretion of the Russian president. To date, countermeasures under Federal Law 127-FZ have been taken against Ukraine, the United States and the Czech Republic:

- In response to 'unfriendly actions' by Ukraine, Presidential Decree 592 of 22 October 2018 and Government Order 1300 of 1 November 2018 imposed the first measures under Federal Law No. 127-FZ. The assets (non-cash funds, non-documentary securities and property) of currently 849 individuals and 84 companies – almost all of them Ukrainian – and of the legal entities controlled by them that are located in Russia have been blocked or frozen. It is also prohibited for their funds to be transferred out of Russia. On 23 October 2020, the State Duma adopted Draft Law 996800-7 at its first reading, which regulates the practical implementation of the asset freeze; this Draft Law is likely to become law.
- Based on Federal Law 127-FZ, Presidential Decree 243 of 23 April 2021 and Government Order 1230-r of 13 May 2021 imposed certain restrictions regarding the employment of individuals located in Russia by diplomatic and consular bodies, as well as representative offices of state authorities and state bodies of 'unfriendly states', namely the Czech Republic and the United States.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

In 2018, the Russian Federation introduced for the first time comprehensive sanctions in the form of countermeasures to respond to sanctions by the United States and the European Union. This response was triggered mainly by the adoption of the US Countering America's Adversaries Through Sanctions Act on 2 August 2017 and the extension of the US sanctions on 6 April 2018. These countermeasures are a combination of economic sanctions and measures to prevent the implementation of US and EU sanctions in Russia.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Not applicable.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

On 15 May 2018, the State Duma adopted at its first reading a draft blocking law that provides for criminal liability with a penalty of up to four years' imprisonment for any Russian or non-Russian individual who complies with foreign sanctions and thereby

© Law Business Research 2021

restricts the ordinary business operations of Russian persons. In addition, deliberate actions by Russian individuals that facilitate the introduction of foreign sanctions against Russian persons shall be punished by up to three years' imprisonment. Currently, this legislative initiative has been put on hold.

However, Russia has adopted other legislation that aims to prevent the implementation of US and EU sanctions in Russia.

Throughout 2018, the Russian government issued orders restricting the disclosure of information relating to sanctioned persons. Information available from public sources may now be incomplete with respect to sanctioned persons. Apparently, these restrictions are designed to protect the business partners of sanctioned persons from the consequences of sanctions violations.

On 19 June 2020, changes to the Russian Arbitrazh (Commercial) Procedural Code came into force, which establish a specific jurisdiction in Russia for any disputes with the participation of listed Russian persons as well as foreign legal entities that have been listed because of sanctions imposed on Russian persons. In certain circumstances, these disputes now fall into the exclusive competence of the Russian commercial courts. To enforce the new rules on specific jurisdiction in Russia, the Russian court may order the counterparty to pay a penalty to the protected listed person. As a result, in many cases, listed Russian and foreign persons (as well as parties in disputes having their basis in sanctions against Russian persons) may be able to transfer their dispute to a Russian commercial court.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Since 2018, Russian courts have developed case law that aims to prevent the implementation of US and EU sanctions in Russia. Two court decisions stand out.

On 13 February 2018, the Russian Constitutional Court issued a landmark decision on parallel imports in which it stated in an *obiter dictum* that 'compliance with a sanctions regime against the Russian Federation . . . can by itself be viewed as bad-faith conduct'. Since the Russian Civil Code obliges all parties to exercise their civil law rights in good faith, the court's position may render unenforceable any sanctions clauses in agreements governed by Russian law (e.g., rights to terminate an agreement if the Russian counterparty becomes sanctioned).

In *Siemens v. Technopromexport* (concerning the delivery of gas turbines to Crimea), the Ninth Commercial Appellate Court stated in its dismissal of Siemens' appeal on 10 April 2018 that:

> *the main consequence of granting the appeal would be the de jure application of economic sanctions imposed by the European Union on the territory of the Russian Federation (i.e., the acknowledgement by the court that Russian legal entities have an obligation to comply with them), which would clearly contradict the fundamentals of the legal system of the Russian Federation (public order) – and cause damage to the sovereignty of the state.*

Since an action that is contrary to public order can be a ground for refusing the recognition of foreign arbitral awards in Russia, this position may render unenforceable any arbitral awards based on the exercising of rights under sanctions clauses.

© Law Business Research 2021

Owing to recent legislative changes that establish a specific jurisdiction in Russia for sanctions-related disputes, foreign corporations may be faced with this court practice more often when trying to enforce claims against listed persons or rights under sanctions clauses. This applies in particular when the foreign corporation owns assets in Russia, or the court decision or arbitral award would have to be enforced in Russia. It is even more important, therefore, to draft sanctions clauses carefully in each case, taking into account applicable Russian court practice.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Misconduct is most often revealed by external and internal whistleblowers. Most whistleblowers do not simply allege violations, they accuse specific employees or the management of the Russian company of personal misconduct. Usually, the main trigger for reporting an actual violation is a personal grudge or the intention to harm a workplace rival. Further, employees often do not sufficiently trust the local management. Many whistleblowers thus prefer to report anonymously, which makes it harder to assess the allegations. However, these anonymous whistleblowers may be as credible as those who disclose their identity.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Yes, the processing of any personal data of Russian citizens triggers the application of Federal Law 152-FZ 'On Personal Data' of 27 July 2006. Under this law, personal data is defined as 'any data that relates directly or indirectly to an individual who can be identified by this data'. The processing actions that trigger the application of the law are recording, systematising, aggregation, storage, specification (updating and modification) and extraction of personal data.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Russian data protection authority, Roskomnadzor, performs its own monitoring of data breaches (including monitoring the internet and relevant news). Roskomnadzor also actively responds to complaints that, in practice, can be filed by data subjects, prosecutors or competitors. Following a complaint or based on the results of its own monitoring, Roskomnadzor can perform a non-scheduled audit, giving a company only 24 hours' prior notice of the audit.

Roskomnadzor also performs a substantial number of scheduled audits. The relevant schedules are published on the official websites of the relevant territorial subdivisions of Roskomnadzor at the beginning of each calendar year. As a result of such an audit, Roskomnadzor can issue an order to remedy a breach or institute administrative proceedings before a court.

© Law Business Research 2021

Roskomnadzor performs more audits of corporations in industries that are considered more risky from a privacy angle. For example, in 2020, Roskomnadzor mostly concentrated on banks (OTP Bank and Russian Standard Bank), airlines (Aeroflot and Nordwind), insurance companies (Ingosstrakh) and a few subsidiaries of multinational companies (General Electric, KIA and Alibaba). Roskomnadzor also took action against companies that do not have a presence in Russia (such as Facebook and Twitter).

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The processing of personal data requires the consent of the relevant employee. Usually, there are no statutory exemptions from the consent requirement that apply to an internal investigation. In particular, according to the current practice of Roskomnadzor, the corporation may not argue that the processing of the personal data is necessary for the exercise of its rights or legitimate interests. Since the employee must consent to the transfer of data to each specific data recipient, all participants in the investigation must be named in the consent. Even stricter requirements apply to data transfer to countries such as the United States, which are not considered to provide adequate protection to personal data. The consent to such data transfer must be issued in writing (ink on paper). Problems can be caused if the employee revokes his or her consent.

In addition, the employing company and each specific data recipient must enter into a data transfer agreement that stipulates that the data recipient will ensure at least the same level of data protection as applied by the Russian company. A separate Russian law agreement is generally advisable.

The cross-border transfer of personal data must also comply with data localisation requirements. In particular, the Russian database must be the primary one and a foreign database could be either a partial or a full (mirroring) copy of the Russian primary database.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The review of emails and computers of employees in Russia is allowed if the employee agrees to the relevant procedures and, most importantly, to the access to his or her communications. This agreement may be given either in (1) a handwritten consent, (2) the employment contract or (3) an internal policy of the company under which the employee puts an ink signature confirming his or her acknowledgement and consent. Otherwise, the company may face potential criminal accusations for the breach of privacy of communications or for illegal access to computer information containing information about an employee's private life or family secrets.

© Law Business Research 2021

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Russian law enforcement authorities at the federal, regional and municipal levels conduct audits of companies quite frequently. The procedures for these audits are regulated by various laws that set out in detail the rights and obligations of the company and the relevant authority. The general principles are laid down in Federal Law 294-FZ 'On the protection of legal entities during the exercise of state control'.

Companies can be targeted by 'scheduled' and 'non-scheduled' audits (i.e., dawn raids). Scheduled audits are conducted according to annual schedules, a consolidated version of which is published on the website of the General Prosecutor's Office until 31 December of the preceding year. Non-scheduled audits are conducted based on specific grounds and must usually be notified to the company at least 24 hours in advance. In most cases, both types of audits are conducted in the form of a request for documents or an on-site visit to the company's premises (or both). An audit must not take longer than 20 business days.

An audit can only be conducted on the basis of a written order, which must comply with certain formal requirements and has been issued by the head or deputy head of the relevant authority. The authority must document the results of the audit in detail in a written report in two original copies, one of which must be handed over to the company. Objections regarding the content of the audit report must be submitted to the relevant authority in writing within 15 calendar days. Other decisions, actions or inaction of the authority in connection with the audit must be challenged in a Russian state court.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

There is no general attorney–client privilege, according to Western understanding, under Russian law. Only certain work-product of specially licensed attorneys (advocates) enjoys limited protection from seizure by 'advocate secrecy'.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Each individual is generally obliged to provide testimony as a witness in administrative and criminal proceedings (Administrative Offences Code, Article 25.6.(2); Criminal Procedural Code, Article 56(6.)(2)). Refusal to provide testimony may entail criminal liability (Criminal Code, Article 208). According to Article 51 of the Constitution of the Russian Federation, an individual is not obliged to provide testimony against himself or herself, his or her spouse or close relatives. If the individual voluntarily provides testimony, he or she must be warned that the testimony can be used as evidence in a criminal case (Criminal Procedural Code, Article 56(4)(1)).

© Law Business Research 2021

There are no comparable provisions that would protect corporations in administrative proceedings against them.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Article 9(4) of the Anti-Corruption Law states that public officials who report on corruption violations are protected by the state in accordance with Russian law. The law therefore only confirms that whistleblowers in the public sector enjoy the protection of the general rules of, for example, Federal Law 45-FZ 'On state protection of judges, officials of law enforcement bodies . . .', Federal Law 119-FZ 'On state protection of victims, witnesses and other participants of criminal court proceedings' and the Criminal Procedural Code. In addition, Presidential Decree 309 dated 2 April 2013 provides for some restrictions on the taking of disciplinary measures against state employees who report corruption.

Even less protection is granted to whistleblowers reporting corruption who are employed in the private sector. Except for a general provision of Presidential Decree 309 dated 2 April 2013, according to which citizens shall be granted legal aid when preparing to report corruption, they are only protected by the general rules of criminal procedural law. A draft law that provided for extensive protection of whistleblowers reporting on corruption in the public and private sectors, and which already had been adopted by the State Duma at its first reading on 13 December 2017, was ultimately rejected on 19 June 2019. In the foreseeable future, therefore, whistleblowers in the private sector can rely only on the protection granted by their employers in accordance with applicable internal rules.

Irrespective of the insufficient whistleblower protection, the Russian state is trying to encourage whistleblowing with monetary rewards. Since 28 August 2018, the Russian Ministry of the Interior is authorised to pay individuals who report on crimes, including bribery and corruption, rewards that may exceed 3 million roubles, according to Order 356 of the Ministry of the Interior dated 6 June 2018.

In contrast to reporting channels established by the state, reporting channels of multinational companies for Russia may violate the Russian data localisation requirements. In particular, this is the case where, upon the receipt of reports, personal data of Russian citizens are collected and saved for the first time outside Russia. Reporting channels with foreign telephone numbers, as well as email addresses or websites with data storage on servers abroad, are therefore not permitted. That means that group-wide whistleblowing systems cannot be extended to Russia without problems.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Except for potentially applicable whistleblower protection, employees, including officers and directors, do not have any special rights under Russian employment law during internal or external investigations.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

A company can apply disciplinary measures against employees who have engaged in misconduct only in compliance with the strict requirements of the Labour Code. Disciplinary measures for a specific violation must be imposed within a month of the violation being uncovered. There is also an overall limitation period for disciplinary measures, which commences when the violation occurs. In practice, these limitation periods – in particular the one-month period commencing on the date of discovery of the violation – prevent the company in many cases from taking disciplinary actions against employees who have violated their labour duties and, in some cases, even committed administrative or criminal offences. To apply disciplinary measures, the company must obtain and properly document the investigation results prior to the expiry of these limitation periods.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Employees must participate in an internal investigation only to the extent that the required action falls within the scope of their labour duties such as, for example, the provision of documents and information to the company's management. A one-time refusal to take such action, however, is unlikely to constitute a ground for dismissal under the very employee-friendly Labour Code. Employees are free to choose whether or not to take any action outside the scope of their labour duties (e.g., whether to participate in interviews with external advisers).

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

In many Russian companies, internal investigations are conducted on an ad hoc basis by the company's security department, which is staffed by former military and police personnel. Therefore, the practice of preparing an investigation plan can rather be found in international law firms that assist multinational companies in internal investigations at their Russian subsidiaries.

The investigation plan would set out the major investigation steps as well as timing and responsibility for the relevant steps. At the initial stage of an investigation, the plan would typically include the following steps:

- examination of the whistleblower's report and correspondence with the whistleblower;
- preliminary analysis of potential liability risks;
- preservation of emails and hard copy documents;
- preparation of documentation required for compliance with data protection requirements;
- background interviews with local personnel and management;

© Law Business Research 2021

- e-search and review of hard copy documents;
- interviews with employees who are suspected of misconduct, during which evidence is presented;
- implementation of disciplinary measures; and
- communication with local management and other logistical issues.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

The company should conduct an internal investigation to clarify the issue, take the required disciplinary measures against employees who have engaged in misconduct, ensure that any established violations are treated with strict confidence within the company, and improve the company's compliance management system to avoid repeated violations. Additional internal steps such as, for example, reporting to a group-wide compliance department, may be required according to the company's internal regulations.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Documents and information must be requested by the Russian law enforcement authorities based on written requests that specifically list the requested material. The material must be provided within a limited period which, in some cases, may not be more than a few business days. Failure to meet the deadline may entail administrative liability of the company and its management. Therefore, immediately upon receipt of the request, the company's management should instruct a senior employee to collect the requested materials. The collected materials should be provided to the authorities by the relevant deadline in strict compliance with all formal requirements.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

The company is generally not obliged to publicly disclose internal investigations or the fact that it has been contacted by the authorities.

37 How are internal investigations viewed by local enforcement bodies in your country?

The concept of internal investigations according to Western understanding is foreign to Russian law. Russian law enforcement authorities have not imposed any requirements regarding the conduct or format of such internal investigations.

© Law Business Research 2021

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

There is no general attorney–client privilege under Russian law. Only information connected to the provision of legal services by specially licensed attorneys (advocates) to their clients is protected. This information falls under what is known as advocate secrecy. Therefore, internal investigations can be protected by advocate secrecy only to the extent that they are conducted by advocates.

Given the limited scope of advocate secrecy, the onus is usually on the investigators to take practical measures to protect the investigation results. Apart from that, the investigators must consider what is required to maintain privilege protections under other jurisdictions – in particular the US attorney–client privilege.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The protection afforded by advocate secrecy is rather limited:

- An advocate (a specially licensed attorney) cannot be called or questioned as a witness regarding facts that became known to him or her in connection with his or her legal services.
- Law enforcement authorities may search the advocate's premises only on the basis of a court order.
- The advocate's work-product that has been obtained during a search is barred from being used as evidence for the prosecution.

There are no differences when the client is an individual.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Advocate secrecy does not usually apply to in-house counsel. The reason for this is that the advocate status entails restrictions that significantly complicate the employment of an advocate in-house. In practice, the status of advocate is therefore obtained only by external counsel.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Under the Advocacy Law, advocate secrecy does not generally apply to advice sought from foreign lawyers practising outside Russia. It is unclear to what extent the privilege applies to foreign lawyers who are registered with the Register of Foreign Lawyers at the Russian Ministry of Justice.

© Law Business Research 2021

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Not applicable.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Not applicable.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Waiving privilege in another country does not affect advocate secrecy in Russia.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Not applicable.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Advocate secrecy extends to any information received by an advocate from third parties in connection with his or her legal services.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

The interviewing of witnesses as part of an internal investigation is not regulated by Russian law.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

The company itself cannot claim privilege over internal witness interviews or attorney reports. Such materials may enjoy the limited protection of advocate secrecy if they constitute certain work-product of advocates (specially licensed attorneys)

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Employees are free to choose whether or not to participate in a witness interview. Most employees, however, will agree to an interview, especially if they are asked to do so by the local company's general director or a representative of the foreign shareholder. Giving warnings to the employee prior to the interview are neither required by law nor widespread

© Law Business Research 2021

in practice. There are also no such requirements when interviewing former employees or other third parties.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Experience shows that the best results can be achieved if the interview is conducted in Russian by a small external team. Documents are presented to the witness as needed. There is generally no need for a lawyer or representatives of a union or workers' council to be involved. Audio or video recording is only permitted with the written consent of the witness.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

The company is generally not obliged to inform the authorities of any misconduct. External advisers of the company, including advocates (specially licensed attorneys), are subject to reporting obligations if there is suspicion of money laundering or terrorist financing. In addition, any individual must report to the law enforcement authorities a limited number of violent offences, such as terrorist activities (Criminal Code, Article 205.6).

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting to exclude or mitigate potential liability is an option available to the company and its representatives for a number of violations under the Administrative Offences Code and the Criminal Code. The self-reporting option for companies to be released from liability for bribery (Administrative Offences Code, Article 19.28: unlawful remuneration on behalf of a legal entity) was only introduced in August 2018. To benefit from self-reporting, it is usually necessary that the authorities have not yet otherwise learned of the violation. However, there are often uncertainties about how to apply the relevant provisions of the law, and fundamental concerns regarding co-operation with the authorities. Therefore, self-reporting in Russia is currently advisable only in exceptional circumstances.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The process of self-reporting is usually not regulated by Russian law and depends on the practice of the relevant law enforcement authority. As a general rule, the benefits of self-reporting by a company will be limited to the reporting company itself. The individuals who committed the violations on behalf or in the interest of the company will

© Law Business Research 2021

still face prosecution under the Criminal Code. However, in some cases, individuals may separately self-report under the leniency provisions of the Criminal Code. Therefore, self-reporting by both the company and its representatives may have to be harmonised.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

In Russian practice, the law enforcement authorities are generally considered to be adversaries of the company. Therefore, on the one hand, the company will fully comply with the notice or subpoena from the authority. On the other hand, the local management will take measures to protect the company's interests against potential hostile actions by the authority. The protective measures to be taken differ depending on the investigating authority and the type of violation being investigated.

55 Are ongoing authority investigations subject to challenge before the courts?

As a general rule, legal acts, decisions, actions or inaction of the law enforcement authorities in connection with an investigation that violate the rights or legal interests of a company, and do not comply with Russian legislation, can be challenged in a Russian state court.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Owing to the different priorities of Russian law enforcement and the general absence of co-operation with its Western counterparts, parallel investigations by Russian and foreign authorities regarding the same facts or allegations currently are very unlikely. Should such a situation arise, the company should handle the Russian investigation separately from the foreign investigation.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The company must provide any material requested by the Russian law enforcement authority, including material located or issued in other countries. Documents issued in other countries must be provided with an apostille and a certified translation into Russian.

© Law Business Research 2021

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Russian law enforcement authorities can request and provide legal assistance on the basis of the treaties on mutual legal assistance entered into with other countries, including many European countries (e.g., according to the European Convention on Mutual Assistance in Criminal Matters of 1959) and the United States (e.g., according to the Treaty Between the Russian Federation and the United States of America on Mutual Legal Assistance in Criminal Matters of 1999). In practice, however, information and investigative materials are shared with foreign authorities only in exceptional cases.

The purpose of legislative changes that entered into force at the end of 2019 is to enable the increased prosecution of foreign companies for bribery offences committed in or outside Russia. If the prosecutor's office sends a letter rogatory to a foreign authority in the course of an investigation, the duration of the administrative investigation can be extended from the previous maximum of two months to 12 months. In the current political climate, it is certainly questionable whether these legislative changes will indeed lead to intensified co-operation by Russian law enforcement agencies with their foreign counterparts.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

The Russian law enforcement authorities must process protected information (such as state secrets, commercial secrets and official secrets) that they receive during an investigation in accordance with secrecy regimes established by Russian law (in particular, by Law RF 5485-1 'On the state secret' and Federal Law 98-FZ 'On the commercial secret').

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should provide to the Russian law enforcement authority a letter from a law firm in that country, which confirms that the production of the documents would violate local law. To be accepted by the Russian authority, the letter should be provided with a certified translation into Russian.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Not applicable.

© Law Business Research 2021

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The voluntary provision of material to the Russian law enforcement authorities may violate contractual confidentiality obligations towards third parties. Material provided to Russian authorities, whether compelled or voluntarily, is generally not discoverable by third parties. The authorities must keep provided material confidential to the extent that it is protected by secrecy regimes established by Russian law (in particular, the state secret regime and the commercial secret regime).

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Under the Administrative Offences Code, companies generally may face fines, confiscation of the instrument of the administrative offence and suspension of operations. Directors and officers of the company are liable under the Administrative Offences Code to fines and occupational bans from certain professions. Any employee of the company may face penalties under the Criminal Code, including fines, occupational bans and imprisonment.

For example, for the commission of offences under Article 19.28 of the Administrative Offences Code (unlawful remuneration on behalf of a legal entity), the following penalties may be imposed on a company:

- minimum: penalty of up to three times the amount of the bribe sum, but not less than 1 million roubles;
- large-scale bribery: if the bribe sum exceeds 1 million roubles, a penalty of up to 30 times the bribe sum, but not less than 20 million roubles; and
- extra large-scale bribery: if the bribe sum exceeds 20 million roubles, a penalty of up to 100 times the bribe sum, but not less than 100 million roubles.

Money, securities or other property, valuable services or other property rights that had been transferred, offered or promised shall be confiscated from the company.

In addition, companies convicted of bribery are being included in a blacklist, which is published on the website of the General Prosecutor's Office. Listed companies are excluded from state procurement processes for two years.

Individuals who commit a bribery offence on behalf or in the interest of a company may face fines, occupational bans and imprisonment under the various bribery offences of the Criminal Code; for example, a bribe given to a domestic public official (Article 291) or commercial bribery (Article 204).

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Not applicable.

© Law Business Research 2021

65 What do the authorities in your country take into account when fixing penalties?

When imposing penalties under the Administrative Offences Code, the courts and authorities shall take into account the financial situation of the company as well as any circumstances that mitigate or aggravate the administrative liability. In general, the fines imposed on companies for corporate misconduct are much lower than those imposed in Western countries.

For example, the fines that are usually imposed by the courts on companies for bribery and corruption are low, not only compared with other countries. They are also well below the maximum fines under Russian law, which may range up to 100 times the bribe sum. Most companies have to pay only the statutory minimum fine of 1 million roubles. The reason for this is the preference of the prosecutor's offices for prosecuting smaller companies on which even the minimum fine of 1 million roubles can have a crippling effect. In many cases, the courts have to decrease even the minimum amount owing to financial difficulties on the part of the companies being fined.

According to information published by the General Prosecutor's Office, however, the amount of the maximum fine imposed for corporate bribery during the year increased significantly, from 30.5 million roubles in 2018 to 50 million roubles in 2019 and 59.8 million roubles in 2021. In 2019, the court of first instance imposed a fine of 100 million roubles in addition to the confiscation of the 56 million roubles bribe. This indicates that higher fines are not inconceivable.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Not applicable.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Not applicable.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Not applicable.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Not applicable.

© Law Business Research 2021

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Not applicable.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under Russian law, companies can be held liable for corporate misconduct under the Administrative Offences Code. Information about scheduled audits of companies is published on the website of the General Prosecutor's Office and the law enforcement authorities conducting the relevant audit. Further, some law enforcement authorities – such as the Federal Antimonopoly Service (FAS) and the Russian data protection authority, Roskomnadzor – may publish information about the opening of administrative cases on their website. Once a company has been convicted of an administrative offence, information about the case can be obtained from published court decisions, press releases of the law enforcement authorities and public registers of offenders.

For example, companies convicted for corporate bribery are included on a blacklist that is published on the website of the General Prosecutor's Office. In 2020 alone, this blacklist gained 325 new entries. For companies with international operations, being included on the blacklist not only results in a loss of reputation; it may also expose companies to additional prosecution risks outside Russia.

The actual purpose of the blacklist is to exclude punished companies from state procurement processes for two years. However, there is currently no automated procedure by means of which the data of excluded companies are transferred to the authorities responsible for state procurement. Therefore, as the results of an investigation initiated by the General Prosecutor's Office show, this exclusion is still not always properly enforced in practice. In 2019, for example, 22 blacklisted companies were able to enter into procurement contracts in 36 Russian regions.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In most cases, corporate communications in Russia are managed in-house directly by the company's management and without instructing a public relations firm.

73 How is publicity managed when there are ongoing related proceedings?

In most cases of ongoing related proceedings (e.g., criminal investigations against individuals), publicity is usually managed directly by the company's management.

© Law Business Research 2021

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Russian law does not generally provide for settlements in administrative proceedings against companies.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

On 12 July 2021, the Bank of Russia issued 'Recommendations for the disclosure of non-financial information . . .'. These recommendations encourage public joint stock companies, which are regulated by the Bank of Russia, to publicly disclose information about how they take into account ESG factors and implement them into their business model and development strategy.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

On 2 July 2021, the State Duma adopted Federal Law 296-FZ 'On the reduction of greenhouse gas emissions' ,which will enter into force on 30 December 2021. This Law sets out the legal basis for further regulation of economical and other activities so as to reduce the emission of greenhouse gases in Russia.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Russia has started to adopt legislation addressing ESG matters only very recently. Therefore, so far there has been no increase in related enforcement activity.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

We are currently not expecting to see any key regulatory or legislative changes emerge that are designed to address corporate misconduct. In particular, the National Anti-Corruption Plan for 2021 to 2024, which was adopted by the Russian president on 16 August 2021 to coordinate the efforts to combat corruption in Russia, does not provide for such changes.

© Law Business Research 2021

21

Singapore

Kabir Singh, Janice Goh and Tian Yi Tan[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

There are currently no high-profile investigations under way in Singapore. The most recently concluded major corporate investigations are those in respect of the corruption scandal involving 1Malaysia Development Berhad (1MDB) and those concerning Keppel Offshore & Marine (Keppel O&M, a subsidiary of Keppel Corporation) and its involvement in the Petrobras bribery scandal.

In relation to 1MDB, the Monetary Authority of Singapore (MAS) conducted a review from 2015 to 2017 of banks involved in 1MDB-related transactions. Two banks have been shut down and total financial penalties of S$29.1 million have been imposed on eight banks for various breaches of anti-money laundering requirements. Goldman Sachs Group Inc has entered into a deferred prosecution agreement (DPA) with the United States Department of Justice. The DPA provides for a global resolution; as part of the DPA, Goldman Sachs (Singapore) Pte Ltd will pay US$122 million to the Singapore government for its role in the 1MDB bond offerings.

Various individuals have been sentenced by the Singapore courts or were served prohibition orders or notices of intention by the MAS prohibiting them from (1) performing any regulated activity under the Securities and Futures Act (SFA) or the Financial Advisers Act (FAA) and (2) taking part, directly or indirectly, in the management of, acting as a director of, or becoming a substantial shareholder of, any capital market services or financial advisory firms under the SFA or the FAA.

1 Kabir Singh is a partner at Clifford Chance Asia. Janice Goh is a partner and Tian Yi Tan is a senior associate at Cavenagh Law.

© Law Business Research 2021

Separately, Keppel O&M has reached a global resolution with criminal authorities in the United States, Brazil and Singapore in relation to corrupt payments made by a former agent in Brazil to officials of Brazilian state-run oil company Petrobras and other parties, to win contracts with Petrobras or its related companies. The corrupt payments were allegedly made with the knowledge or approval of former Keppel O&M executives. As part of the resolution, Keppel O&M is subject to fines amounting to US$422.2 million, to be allocated between the United States, Brazil and Singapore.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held criminally liable in Singapore. Under the Interpretation Act, which governs the interpretation of all Singapore law statutes generally, 'person' includes any company or association or body of persons, corporate or unincorporate. Under the Penal Code, which is the main criminal law statute in Singapore, the word 'person' includes any company or association or body of persons, whether incorporated or not.

Specific statutes also contain provisions attributing liability to corporations and their officers. For example, under section 59 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, where an offence under the Act committed by a body corporate is proven to have been committed with the consent or connivance of an officer, or to be attributable to any neglect on his or her part, both the officer and the body corporate will be guilty of the offence and shall be liable to be proceeded against and punished accordingly. Similar provisions are found in other statutory legislation, such as the SFA.

In *Ho Kang Peng v. Scintronix Corp Ltd* [2014] 3 SLR 0329, the Singapore Court of Appeal referred to the three rules of attribution to determine when an act by a person representing a company can be attributed to the company. These rules applied to any person representing the company (1) primary rules of attribution, that is the company's constitution, (2) general rules of attribution, that is, the principles of agency, and (3) special rules of attribution, that is, the court will determine, on construction of the statutory provision, whether it is intended to include the acts of such an individual as the act of the company.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The law enforcement authorities that regulate corporations include the following:

- Accounting and Corporate Regulatory Authority, the national regulator of business entities, public accountants and corporate service providers;
- MAS, which is Singapore's central bank and is focused on enforcement issues relating to financial institutions and the financial services and securities industries;
- Inland Revenue Authority of Singapore, the tax authority in Singapore;
- Competition and Consumer Commission of Singapore, which exercises oversight over competition-related matters; and
- Personal Data Protection Commission, which exercises oversight over data privacy matters.

© Law Business Research 2021

More generally, the Commercial Affairs Department (CAD), a division of the Singapore Police Force, and the Corrupt Practices Investigation Bureau also exercise oversight over the acts of corporations. These entities have statutory powers to investigate and prosecute offences relating to bribery, corruption and other financial and white-collar crimes.

The MAS and CAD are parties to a joint investigation arrangement, under which they jointly investigate all offences under the SFA and the FAA, to allow both agencies to consolidate their investigative resources and expertise and further improve the overall effectiveness of market misconduct investigations.

Jurisdiction among the authorities is allocated in terms of subject matter generally. General procedures on the prosecution of individuals and corporations are set out in the Criminal Procedure Code and supplemented by provisions within various statutes. In practice, to streamline the process, investigations are usually only commenced by one authority unless there are common issues of relevance to more than one authority (for example, in a case of fraud, the CAD may investigate the fraud alongside the MAS, which may be involved in money laundering issues to the extent that the fraudulent monies were transferred via banks in Singapore).

In addition to the aforementioned law enforcement authorities, there are self-regulatory organisations (SROs) that perform some regulatory functions. For example, in the area of securities and derivatives trading, the approved exchanges (such as the Singapore Exchange Securities Trading Limited) are SROs, with rules governing both their members (business rules) and listed companies (listing rules). The approved exchanges are responsible for administering their respective listing rules, exercising supervision over their members, and ensuring fair and orderly trading of their listed products.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

There is no specific threshold of suspicion necessary to trigger a police investigation.

Also, there is no specific threshold of suspicion set out in legislation necessary for the MAS to initiate an investigation into an alleged or suspected contravention. For example, under the SFA, the MAS may initiate an investigation so long as it considers an investigation 'necessary or expedient' (SFA, section 152).

In practice, each authority is likely to prioritise its resources in considering how to respond to all potential breaches of law and whether to undertake a formal investigation. For example, the MAS will consider a range of factors to determine whether to undertake a formal investigation, including the seriousness of the misconduct, the public interest in pursuing the misconduct and the availability of evidence required to prove the misconduct.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A notice or subpoena from a law enforcement authority may be challenged by asking the court to quash it or prohibit further action by the relevant law enforcement authority.

A search warrant issued by the Singapore courts under the Criminal Procedure Code may be suspended or cancelled if there are valid grounds for doing so.

© Law Business Research 2021

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Singapore has a framework for deferred prosecution agreements (DPA). This enables corporates to reach agreement with the Public Prosecutor for the deferral of prosecution, in exchange for the imposition of certain requirements.

7 What are the top priorities for your country's law enforcement authorities?

Generally, the top priorities for Singapore's law enforcement authorities include corruption, financial crimes and cybercrime, and for financial institutions, market abuse, financial services misconduct and money laundering-related control breaches.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

The presence of an effective compliance programme is usually a mitigating factor, in terms of the quantum and severity of the penalties to be imposed on a corporation.

Under the DPA framework, authorities may defer prosecution on the basis that the company agrees to certain conditions, including putting in place certain compliance frameworks.

Certain authorities have published guidance about what constitutes an effective compliance programme; for example, the Corrupt Practices Investigation Bureau developed 'PACT: A Practical Anti-Corruption Guide for Businesses in Singapore' to help domestic business owners prevent corruption in their companies. The MAS has published 'Guidelines on Risk Management Controls', which facilitate the implementation of an effective compliance programme.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Cybersecurity and data security issues are primarily regulated through the Cybersecurity Act 2018 (CSA) and the Personal Data Protection Act (PDPA).

The key objectives of the CSA are to (1) strengthen the protection of critical information infrastructure (CII) against cyberattacks, (2) authorise the Cyber Security Agency to prevent and respond to cybersecurity threats and incidents, (3) establish a framework for sharing cybersecurity information, and (4) establish a light-touch licensing framework for cybersecurity service providers. The CII sectors are energy, water, banking and

© Law Business Research 2021

finance, healthcare, transport, audiovisual communications, media, security and emergency services, and government.

The PDPA provides a baseline standard of protection for personal data. It complements sector-specific legislative and regulatory frameworks, such as the Banking Act and the Insurance Act. It comprises various requirements governing the collection, use, disclosure and care of personal data.

As of 1 February 2021, amendments to the PDPA introduced a mandatory data breach requirement. If an organisation identifies a notifiable data breach, the breach must be reported to the Personal Data Protection Commission (PDPC). The organisation must also notify affected individuals once the organisation has determined that the data breach is likely to result in significant harm to any individuals to whom the information relates.

In 2018, SingHealth (Singapore's national healthcare service provider) was affected by a major data breach involving compromise of the personal particulars of 1.5 million patients and records of outpatient dispensed medicines belonging to 160,000 patients. A committee of inquiry was convened on 24 July 2018 to investigate the causes of the attack and identify measures to help prevent similar attacks. The incident was attributed to sophisticated unnamed state-linked actors. In January 2019, the PDPC imposed fines of S$750,000 on Integrated Health Information Systems (the central information technology agency responsible for Singapore's healthcare sector) and S$250,000 on SingHealth for breaching its data protection obligations under the PDPA. These financial penalties are the highest imposed by the PDPC to date.

In addition to the CSA and the PDPC, the Monetary Authority of Singapore (MAS) also issues notices and guidelines in relation to cybersecurity for financial institutions, such as the MAS Technology Risk Management Guidelines and Notice on Cyber Hygiene.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Yes, cybercrime is regulated in Singapore under the Computer Misuse Act. Cybercrime is a serious criminal offence, which is investigated by the Singapore Police Force.

At the regional level, Singapore is the Association of Southeast Asian Nations (ASEAN) Voluntary Lead Shepherd on Cybercrime. This provides a platform for the ASEAN Member States to coordinate the regional approach to cybercrime, and work together on capacity building, training and the sharing of information.

At the international level, Singapore hosts the Interpol Global Complex for Innovation (IGCI), Interpol's global hub on cybercrime. Singapore has led the IGCI Working Group and the Interpol Operational Expert Group on Cybercrime, working with other Interpol Member States to define Interpol's cybercrime programme.

© Law Business Research 2021

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In the main, local criminal law does not have general extraterritorial effect. However, in relation to certain specific offences, extraterritoriality may apply; for example, Singapore citizens committing corruption or bribery overseas may be charged under the Prevention of Corruption Act. The Terrorism (Suppression of Financing) Act is another example of legislation with extraterritorial effect.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Principal challenges arising in cross-border investigations include those concerning the collection of evidence and the implementation of enforcement action.

Most of the time, these matters are dealt with between governments pursuant to treaties on mutual legal assistance between the jurisdictions involved, which are given legal effect under the Mutual Assistance in Criminal Matters Act.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

It is unclear whether the concept of international double jeopardy applies in Singapore, as the issue has not been tested in Singapore courts.

That said, double counting is prohibited insofar as breaches of Singapore law are concerned. Section 40 of the Interpretation Act (Cap. 1) states that where any act or omission constitutes an offence under two or more written laws (i.e. legislation in Singapore), the offender shall, unless the contrary intention appears, be liable to be prosecuted and punished under any one of those written laws but shall not be liable to be punished twice for the same offence. Accordingly, multiple authorities will not be able to penalise companies for the conduct insofar as they contravene section 40 of the Interpretation Act.

14 Are 'global' settlements common in your country? What are the practical considerations?

It is not uncommon for there to be 'global' settlements involving the Singapore authorities (e.g., in the *1Malaysia Development Berhad* (*1MDB*) and *Keppel Offshore & Marine/Petrobras* cases). Practical considerations include the level of co-operation amongst the authorities in the various jurisdictions.

© Law Business Research 2021

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Generally, in practice we expect that regulators will ordinarily seek to achieve consistency where practicable, particularly when co-operating with foreign authorities.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Singapore implements United Nations Security Council sanctions through the United Nations Act (Cap. 339) for non-financial institutions and individuals and the Monetary Authority of Singapore Act (Cap. 186) for financial institutions.

Singapore also applies targeted financial sanctions against designated individuals and entities under the Terrorism (Suppression of Financing) Act. The relevant individuals and entities are designated by the Inter-Ministry Committee on Terrorist Designation pursuant to the United Nations (UN) Security Council Resolution 1373 relating to terrorism.

Singapore does not enforce unilateral sanctions imposed by other countries.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Generally, sanctions implemented in Singapore are enforced by the Singapore Police Force, Singapore Customs (trade sanctions), the Monetary Authority of Singapore (financial sanctions) and the Inter-Ministerial Committee on Terrorist Designation.

The number of prosecutions for sanctions violations has increased over the years. In 2018, T Specialist International and its director, Ng Kheng Wah, were charged in Singapore for, among other things, the supply of sanctioned luxury goods to North Korea in breach of UN sanctions against North Korea. In the same year, Singaporean Chong Hock Yen and North Korean Li Hyin, were charged in court (together with companies linked to Chong) for the supply of perfumes, wines and watches to North Korea in breach of UN sanctions.

In 2020, a Singaporean national on the Federal Bureau of Investigation's most wanted list (Tan Wee Beng) was charged with falsifying invoices of two companies to hide transactions with North Korea-linked entities.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), a mechanism is available for financial intelligence to be shared with other financial intelligence units of other jurisdictions. Assistance may also be provided pursuant to the Mutual Assistance in Criminal Matters Act or the Monetary Authority of Singapore Act.

© Law Business Research 2021

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Singapore does not enforce unilateral sanctions imposed by other countries.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct are often reported by whistleblowers or complainants making complaints directly to companies or to law enforcement authorities or via surveillance of authorities.

Apart from reports or complaints of misconduct, 'suspicious transaction reports' lodged pursuant to disclosure obligations under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) in respect of property that is reasonably suspected of being connected to criminal activity are also a means by which wrongdoing comes to light. These reports are lodged with the Suspicious Transaction Reporting Office, which is Singapore's financial intelligence unit. Although these suspicious transaction reports are property-based and for the purpose of combating money laundering, the Singapore Police Force may also initiate investigations into misconduct associated with the property.

Internal investigations into misconduct may also be initiated pursuant to internal or external audits conducted by a company.

INFORMATION GATHERING

22 Does your country have a data protection regime?

Yes. Personal data is protected under the Personal Data Protection Act (PDPA). The PDPA provides a baseline standard of protection for personal data. It comprises various requirements governing the collection, use, disclosure and care of personal data.

In addition, Singapore has a strict banking secrecy regime under the Banking Act (Cap. 19). Certain other information is also protected under various statutes, such as the Official Secrets Act (Cap. 213). The common law of confidentiality also applies to protect certain types of information.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The PDPA ensures a baseline standard of protection for personal data, which requires organisations to comply with the PDPA as well as common law and other relevant

© Law Business Research 2021

laws that apply to the industry to which they belong, when handling personal data in their possession.

If the Personal Data Protection Commission (PDPC) finds that an organisation is in breach of any of the data protection provisions in the PDPA, it will direct the organisation to take steps to ensure compliance, such as to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to or correct the personal data; and
- pay a financial penalty.

There are also offences under the PDPA for which an organisation or a person may be liable.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

The PDPA provides that an organisation may use or disclose personal data about an individual without the consent of the individual where the use is necessary for any investigation or proceeding.

However, if personal data is to be transferred out of Singapore for the purposes of an internal investigation (e.g., a cross-border investigation), the relevant organisation must comply with the Transfer Limitation Organisation, which requires that an organisation ensure that personal data transferred overseas is protected to a standard comparable with the data protection provisions within the PDPA.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

To the extent that employees' communications contain personal data subject to the PDPA, organisations must comply with the Act in terms of interception of their communications. The PDPA is a consent-based regime, subject to exceptions in the Act. If the organisation is able to rely on an exception to intercept the communications, consent of the employee is not necessary. For example, one of the exceptions in the PDPA is whether the use, collection or disclosure of the personal data is necessary for investigations.

However, if the PDPC finds that an organisation is in breach of any of the data protection provisions in the PDPA, it will direct the organisation to take steps to ensure compliance, for example:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to or correct the personal data; and
- pay a financial penalty.

There are also offences under the PDPA for which an organisation or a person may be liable.

© Law Business Research 2021

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes, search warrants and dawn raids on companies are a feature of law enforcement in Singapore.

Searches are generally conducted by regulatory authorities with search warrants and must be carried out in accordance with the terms within the warrants, as well as any applicable provisions of statutory legislation (e.g., the Criminal Procedure Code). A search warrant may be suspended or cancelled if there are good reasons for doing so (Criminal Procedure Code (CPC), section 27(1)).

There are also instances when searches can be carried out by the police without search warrants, for example, if a police officer has good grounds for believing that stolen property will be removed from the premises by the time the search warrant is obtained.

If an illegal search is conducted, the aggrieved party may make a criminal complaint for trespass or criminal force, or commence a civil claim for damages in the tort of trespass.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

A company subject to a search and seizure order should inform investigating officers that there is (or may be) privileged material within the seized data and assert its claim to privilege. Thereafter, it should follow up with a written notice to claim privilege and reserve all its rights.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

There are statutory provisions that allow an individual's testimony to be compelled for the purposes of criminal or regulatory investigations.

For example, section 283(2) of the CPC provides that an individual may be summoned to give evidence when his or her evidence is essential to making a just decision at the close of the case for the defence, or at the end of any proceeding under the CPC.

The Monetary Authority of Singapore (MAS) has the power to require persons to be examined (Securities and Futures Act (SFA), section 154), and evidence obtained by the MAS in this regard may be used in criminal investigations and proceedings (SFA, section 168B).

There is a right against self-incrimination in Singapore under section 22(2) of the CPC, whereby a person need not say anything that might expose him or her to a criminal charge, penalty or forfeiture.

An advocate, solicitor or in-house counsel would be prohibited from disclosing any communications covered by legal privilege (Evidence Act, sections 128 and 128A).

© Law Business Research 2021

Further, a person would not be permitted to produce any unpublished official records relating to the affairs of the state (Evidence Act, section 125).

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Singapore does not have formal whistleblowing legislation. However, whistleblowers may be entitled to protection for the reporting of offences set out within specific statutes (e.g., the Prevention of Corruption Act). Under these statutes, the informer's identity will remain confidential throughout any proceedings that may result from the reporting of the offence.

Companies are also encouraged to maintain internal whistleblowing policies as a matter of corporate governance and best practice.

For example, the Monetary Authority of Singapore, in its Guidelines on Individual Accountability and Conduct, sets out requirements for financial institutions to maintain a formalised whistleblowing programme. The programme should include the whistleblowing channels available to employees, procedures to ensure anonymity and adequate protection of employees who raise concerns about the financial institution's policies, practices and activities via this channel, and procedures for handling whistleblower complaints.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Section 14(8) of the Employment Act provides that for the purposes of a due inquiry (i.e., conducted as part of the investigations process), an employer may suspend an employee from work for a period not exceeding one week, or such longer period as the Commissioner of Labour may determine on an application by the employer. During the period of suspension from work, the employer must pay the employee at least half of his or her salary. If the inquiry does not disclose any misconduct on the part of the employee, the employer shall immediately restore to the employee the full amount of the salary withheld (Employment Act, section 14(9)).

Under common law, general requirements of due process (a right to a fair hearing, etc.) are applicable.

There is no distinction between officers and directors of the company for these purposes.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Under section 14(1) of the Employment Act, an employee is entitled to a due inquiry before dismissal on the grounds of misconduct. Under common law, general requirements of due process (a right to a fair hearing, etc.) are applicable.

© Law Business Research 2021

Section 14(8) of the Employment Act provides that for the purposes of a due inquiry (i.e., conducted as part of the investigations process), an employer may suspend an employee from work for a period not exceeding one week, or such longer period as the Commissioner of Labour may determine on an application by the employer. During the period of suspension from work, the employer must pay the employee at least half of his or her salary. If the inquiry does not disclose any misconduct on the part of the employee, the employer shall immediately restore to the employee the full amount of the salary withheld (Employment Act, section 14(9)).

32 Can an employee be dismissed for refusing to participate in an internal investigation?

An employee may be dismissed for refusing to participate in an internal investigation, if dismissal for that cause is permitted under the employment contract.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Yes. This document would set out the scope and purpose of the investigation, documents reviewed and referred to, persons to interview, issues in question, impediments to information gathering, as well as an overview of personal data protection laws of which the investigators should be mindful.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

The company should commence an internal investigation. A company should also assess its reporting obligations in respect of the regulatory and law enforcement authorities, and report any suspected or confirmed misconduct as required under applicable legislation.

Typically, as an internal management measure, senior management or the board (or both) would also be briefed, depending on the severity of the conduct involved.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

The company should first assess whether the notice or subpoena applies to it, and whether it is legally obliged to comply with it.

If yes, the company should take steps to comply with the notice or subpoena, which will include imposing document retention notices, finding and preserving data, conducting searches over electronic data sets, among other things. The company should also brief

© Law Business Research 2021

management and the affected employees, and provide instructions regarding compliance with the notice or subpoena.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

This requirement applies only to publicly listed companies. Under the Singapore Exchange (Mainboard) Listing Rules, material information should be disclosed by listed companies. Material information is defined as information that is either 'necessary to avoid the establishment of a false market in [its] securities' or 'that would be likely to materially affect the price or value of its securities'. This information would probably include the existence of an internal investigation or contact from a law enforcement authority.

There is no corresponding disclosure requirement for private companies, although they may wish to voluntarily disclose the matter for public relations purposes and to offset any reputational concerns.

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are generally welcomed as they complement the general law enforcement and regulatory framework. The swift conduct of internal investigations, as well as follow-up reporting to the authorities, may be viewed as a mitigating factor if the authorities decide to press any charges against the relevant company or individuals.

There are no other legal requirements regarding the conduct or format of internal investigations.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal advice privilege and litigation privilege may be claimed over materials and documents generated during internal investigations.

For litigation privilege to apply, there must be a reasonable prospect of litigation at the time the documents were created, and the dominant purpose for the creation of the documents over which privilege is claimed is pending or contemplated litigation. This includes documents that may be generated by third parties (such as forensic accounting reports prepared for the purposes of the internal investigation).

If there is a pending regulatory investigation (which is being conducted in parallel with the internal investigations), a company should record this in writing so that material generated during the internal investigations is more likely to be protected by litigation privilege.

© Law Business Research 2021

For legal advice privilege to apply, it must be shown that the documents in question contain solicitor–client privileged advice, or otherwise was generated for the dominant purpose of seeking legal advice.

For this reason, a company should generally copy its external or in-house legal counsel in on written correspondence generated in the course of internal investigations, and also mark such communications 'strictly confidential and legally privileged' or 'for the purposes of obtaining legal advice'. However, the fact that legal counsel is copied, or that correspondence is marked privileged, does not necessarily mean that the contents of the communications are indeed privileged. A court or tribunal will examine the substance of the communications to determine whether any claims of privilege will succeed.

Further, to mitigate against the risks of disclosure, a company should keep the amount of written communication and documentation generated in an internal investigation to a minimum, and only circulate the materials on a need-to-know basis.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal professional privilege comprises legal advice privilege and litigation privilege. For legal advice privilege to apply, it must be shown that the documents in question contain solicitor–client privileged legal advice, or otherwise was generated for the dominant purpose of seeking legal advice.

For litigation privilege to apply, there must be a reasonable prospect of litigation at the time the documents were created, and the dominant purpose for the creation of the documents over which privilege is claimed is pending or contemplated litigation. This includes documents that may be generated by third parties (such as forensic accounting reports prepared for the purposes of internal investigations).

Privilege is held by the client. There are no material differences in how privilege operates when the client is an individual.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, pursuant to section 131 of the Evidence Act, which expressly provides that in-house counsel are legal professional advisers for the purposes of determining whether privilege applies.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Yes, subject to any additional requirements imposed by the home jurisdiction of the foreign lawyer.

© Law Business Research 2021

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There is no strict legal requirement for waiver of legal professional privilege in the investigations context. However, in practice, if regulatory authorities request privileged information, it may be difficult to reject such a request, as a company will wish to co-operate.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The concept of limited waiver of privilege does exist as a concept in Singapore. In this regard, the English common law position is likely to be endorsed by a Singapore court or tribunal.

The *Belhaj v. DPP* ([2018] EWHC 513 (Admin)) is likely to be persuasive authority on the scope of limited waiver of privilege. In this case, the High Court of England and Wales observed that privilege may be waived for a limited purpose without being waived generally. However, the existence of limited waiver is to be determined objectively and does not depend on the party's subjective intention. Although the Singapore courts have not specifically decided on the issue of limited waiver in the context of limited production to law enforcement agencies, the Singapore courts are likely to view the Hong Kong Court of Appeal decision in *Citic Pacific Limited v. Secretary for Justice and the Commissioner of Police* (CACV60/2011) (whether limited waiver of privilege in respect of documents produced to the Securities and Futures Commission of Hong Kong was recognised) as persuasive authority.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This issue has not been specifically considered or determined in Singapore. However, the concept of limited waiver of privilege is recognised.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists as a concept in Singapore. It can be used to enable one party to shield behind the privilege of another, and prevent a third party from obtaining or using documents disclosed, pursuant to the common interest between the former parties, in the subject-matter of the communications.

For common interest privilege to apply, a 'similar interest' must be at stake. For example, when several persons have a common interest in anticipated litigation, they may be able to assert this privilege.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes. For example, in *Skandinaviska Enskilda Banken AB, Singapore Branch v. Asia Pacific Breweries (Singapore) Pte Ltd* ([2007] 2 SLR(R) 367), the Court of Appeal held that

© Law Business Research 2021

certain draft reports by accountants commissioned by the company's directors after discovery of a fraud on the company were prepared for the dominant purpose of litigation and, therefore, were subject to litigation privilege.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, witness interviews are permitted and are an integral part of an internal investigation.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes. A company can claim legal professional privilege over internal witness interviews or attorney reports, so long as the requirements for legal advice privilege or litigation privilege are satisfied. For legal advice privilege to apply, it must be shown that the documents in question contain solicitor–client privileged legal advice, or otherwise was generated for the dominant purpose of seeking legal advice. Attorney reports, for example, are likely to be protected by legal advice privilege.

For litigation privilege to apply, there must be a reasonable prospect of litigation at the time the documents were created, and the dominant purpose for the creation of the documents over which privilege is claimed is pending or contemplated litigation.

Having a legal counsel attend and conduct witness interviews also enhances the prospects of a claim of legal professional privilege.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no formal legal requirements for the conduct of witness interviews. In practice, *Upjohn* warnings are usually administered at the beginning of a witness interview, and accurate notes of the interview should be taken.

These practical requirements apply equally for interviews of third parties (such as former employees).

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

How an internal interview is typically conducted depends on the internal procedure and policies of the particular company and, therefore, would differ case by case. To facilitate the fact-finding process, documents are usually put to the witnesses at the interview, subject to any confidentiality concerns.

There is no requirement for employees to have their own legal representation, and any request to obtain legal representation at the interview will be subject to the agreement of the employer.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Yes. For example, under section 39 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, if a person knows or has reasonable grounds to suspect that any property is implicated in drug dealing or criminal conduct (i.e., represents the proceeds of a crime, was used in connection with a crime or is intended to be used in connection with a crime), and that knowledge or suspicion arose in the course of his or her trade, profession, business or employment, it must be reported to a Suspicious Transaction Reporting Officer. Failure to do so constitutes a criminal offence.

Under sections 8 and 10 of the Terrorism (Suppression of Financing Act), information about terrorist activity and property must also be disclosed to the police. Failure to do so constitutes a criminal offence.

In the financial services industry, it is mandatory for financial institutions and regulated entities to report certain types of misconduct committed by their representatives under the Monetary Authority of Singapore Notices on Reporting of Misconduct of Representatives by Holders of Capital Markets Services Licence and Exempt Financial Institutions and by Financial Advisers; for example, acts involving fraud, dishonesty or other offences of a similar nature, market misconduct and insider trading, and other types of serious breaches.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Whether a company should self-report to law enforcement even if it has no legal obligation to do so, is a question to be assessed in each particular case. If the misconduct involved is of a nature that would trigger a regulatory investigation, self-reporting would be viewed as a mitigating factor by the regulatory authorities.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Depending on the type of offence or misconduct to be reported, the entity in question should complete a robust internal investigation or review to ensure that the facts are accurate, and that any formal requirements are complied with.

The reporting entity should also envisage questions from the regulator and pre-empt them.

© Law Business Research 2021

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

A company should review the notice or subpoena carefully to determine its scope and legitimacy, and whether the law enforcement authority is properly entitled to the materials sought. If it is, the company should comply with the notice or subpoena (as the case may be).

It is possible to enter into a dialogue with the authorities to address their concerns before, or even after, charges are brought, depending on the facts of the case and the severity of the charges. External lawyers experienced in these matters will typically liaise with the authorities.

55 Are ongoing authority investigations subject to challenge before the courts?

Yes, there is a theoretical risk of judicial review but this is rare in practice.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Yes, it would be prudent for a company to negotiate a consistent disclosure package between the various countries, subject to any applicable local requirements, as regulators will generally expect to be treated fairly and be provided with similar or consistent information.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

This depends on the scope of the subpoena. Generally, if the material is in the possession, custody or power of a company, the company must search for and produce the material. This includes material that may be located overseas (e.g., on a server maintained in another jurisdiction), as long as it is within the possession, custody or power of the company.

When data servers or material are maintained by third parties or related companies not in Singapore and not within the possession, custody or power of the company, it may nonetheless choose to co-operate and offer assistance to provide access to these data servers or materials.

© Law Business Research 2021

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

We expect that law enforcement in Singapore may routinely share information or investigative materials with law enforcement in other countries. These matters are regulated under the Mutual Assistance in Criminal Matters Act, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), the Terrorism (Suppression of Financing) Act and the Monetary Authority of Singapore Act (the MAS Act).

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Certain statutes may contain specific provisions regulating onward disclosure to, and use by, foreign and domestic authorities. See, for example, part VC of the MAS Act, which sets out statutory provisions governing assistance to foreign authorities and domestic authorities for their supervisory and other actions in respect of money laundering, terrorism financing and other offences.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should obtain legal advice explaining why production of those documents would violate the laws of that other country. The company should resist disclosure, providing an explanation as to why production of the documents would cause the company to be in breach of the relevant foreign laws.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Singapore does not have secrecy or blocking statutes, save for the Official Secrets Act, which prevents the disclosure of official government documents and information.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Generally, law enforcement authorities maintain the confidentiality of materials provided to them.

If the documents are privileged, they may be disclosed on the basis of a limited waiver of privilege. If so, this reduces the risk of onward disclosure and use.

© Law Business Research 2021

If the documents are not privileged, the position on onward disclosure to, and use by, third parties is less clear. Foreign law enforcement authorities may request assistance and the sharing of information or documents, pursuant to legislation, treaties or other working agreements between them and the Singapore authorities.

Generally, shareholders will not have a right to apply for disclosure of such documents, unless they are allowed to do so under the company's articles and memorandum of association, or other corporate constitutional documents or agreements, or if they obtain the documents in the course of civil proceedings.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

A company found guilty of a criminal offence will generally be punished by a fine.

A company's directors, officers or employees found guilty of a criminal offence may also be subject to imprisonment or fines (or both).

In this regard, certain legislation (such as section 331 of the Securities and Futures Act) provides that when an offence under the legislation committed by a body corporate is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, an officer of the body corporate, the officer as well as the body corporate shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Further, a company or individual found guilty of a criminal offence may be required by a court to pay compensation to affected third parties.

In addition, companies or their directors, officers or employees may also be subject to sanctions or civil penalties imposed by regulatory bodies such as the Singapore Exchange and the Monetary Authority of Singapore (MAS) (e.g., orders prohibiting or suspending a person from taking part in certain regulated financial activities).

A court may also order a third party who has benefited from misconduct to disgorge the benefit arising from that misconduct, on the application of the MAS or any other claimant, pursuant to section 236L of the Securities and Futures Act.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The options or restrictions applying to such a corporate would depend on the law of that other country. Generally, for certain regulated entities (such as banks and financial institutions), debarment or another regulatory sanction in one country may adversely affect the ability of that entity to carry on similar business in another jurisdiction.

65 What do the authorities in your country take into account when fixing penalties?

The authorities will take into account general sentencing guidelines and sentencing precedents in fixing penalties. They will also consider other factors, such as the severity of the

© Law Business Research 2021

misconduct, the culpability of the offender, whether other mitigating factors exist, the accused person's antecedents, and any other relevant facts relating to the offence.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Deferred prosecution agreements (DPAs) are available for certain offences, including offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, the Prevention of Corruption Act and the Securities and Futures Act. The DPA framework enables corporates to reach agreement with the Public Prosecutor for the deferral of prosecution, in exchange for the imposition of certain requirements.

Further, section 232(5) of the Securities and Futures Act also provides for the possibility of out-of-court settlements with the Monetary Authority of Singapore (MAS), for breach of the disclosure of interests or market conduct provisions in the Act. In such cases, the MAS will expect the person who contravened the relevant statutory provisions to provide an admission of liability (see the MAS Enforcement Monograph, at [6.12]).

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Section 149J of the Criminal Procedure Code provides that the high court may postpone the giving of public notice of matters relating to a DPA as is necessary to avoid a substantial risk of prejudice to the administration of justice in any legal proceedings, investigation under the Criminal Procedure Code, or any criminal investigation under any other written law.

The court also has the power to order that information in court documents be removed or redacted.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies should be aware of any outstanding liabilities that it may have in respect of other parties (e.g., in civil claims) and consider the potential consequences of entering into a settlement agreement with the law enforcement authority. Companies should also consider the effect of a settlement on any pending or parallel regulatory investigations in other jurisdictions, which may arise out of the same or similar subject-matter.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Law enforcement authorities, in particular, the MAS, may use external corporate compliance monitors as an enforcement tool. For example, in April 2021, as part of the

© Law Business Research 2021

enforcement measures taken against Bank J Safra Sarasin Ltd, Singapore Branch for its failures to comply with certain anti-money laundering and counter-terrorist financing requirements, the MAS required the bank to appoint an independent party to validate the effectiveness of the bank's remediation measures and report the findings to the MAS.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

There are no legal restrictions on civil proceedings taking place in parallel with regulatory investigations. However, in practice, civil proceedings are usually put on hold pending the conclusion of criminal proceedings, to avoid conflicting evidence that may complicate the civil proceedings.

Civil litigants are unlikely to gain access to the authorities' files and documents unless special third-party or non-party discovery orders are sought by the litigants and granted by the court.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Criminal cases are generally kept confidential at the investigatory stage, unless there is a public interest in the matter, in which case the relevant authority may choose to issue a press statement stating that it is investigating the matter. However, details of the investigation are unlikely to be released until investigations are complete or certain milestones have been reached.

Once a case is before a court, it will become public knowledge unless any confidentiality orders (e.g., to protect minors) are specifically sought and granted. Generally, and unless ordered otherwise by the court, members of the public may also attend criminal trials.

Under the Administration of Justice (Protection) Act 2016, anyone who intentionally publishes any matter or carries out any other act that prejudices, interferes with or poses a 'real risk of prejudice' to current court proceedings is liable to be found guilty of contempt of court.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Yes, it is common for companies to use a public relations (PR) firm to manage corporate crises in Singapore. A PR firm may work with a company's corporate communications or media relations team to determine the appropriate approach to such communications. Lawyers may also provide high-level input and guidance on these matters.

© Law Business Research 2021

73 How is publicity managed when there are ongoing related proceedings?

Companies generally do not comment on ongoing related proceedings unless it is necessary to do so. In any event, any statements or comment provided by a company must be accurate, unbiased and consistent.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

For listed companies, disclosure may be required under Rule 703 of the Singapore Exchange (Mainboard) Listing Rules, subject to any further requirements imposed by the relevant law enforcement authorities.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

The ESG regulatory regime is developing in Singapore. For example, in 2019, the Monetary Authority of Singapore (MAS) published its Green Finance Action Plan, which sets out strategies for Singapore's transition to green finance.

In 2020, the MAS released a set of Guidelines on Environmental Risk Management for the asset management, banking and insurance sectors. Among other things, these Guidelines require financial institutions to put in place robust policies and processes to manage environmental risk in a systematic and consistent manner (e.g., scenario analysis and stress testing).

Companies listed on the Singapore Exchange (SGX) are also required to submit sustainability reports annually under Listing Rule 711A-B. These reports should cover material ESG factors; policies, practices and performance; targets; a sustainability reporting framework; and a board statement.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

In 2021, the SGX commenced a public consultation exercise on enhancements to its sustainability reporting guidelines, including climate-related reporting in line with the recommendations of the Task Force on Climate-Related Financial Disclosures. This is a first step to better prepare issuers for reporting against anticipated global baseline sustainability reporting standards to be developed by the International Financial Reporting Standards Foundation.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

No, but we expect this to be a rising trend in the future.

© Law Business Research 2021

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The Monetary Authority of Singapore's Guidelines on Individual Accountability and Conduct took effect on 10 September 2021. We expect to see further regulatory scrutiny on the conduct of senior managers and employees of financial institutions, as well as culture and conduct in these institutions more generally.

© Law Business Research 2021

22

Spain

Jaime Alonso Gallo and Sara Sanz Castillo[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Corporate criminal liability was introduced in Spain in December 2010. Since then, there has been a small number of highly significant cases (chief among them being the *Bankia* case, a securities fraud judged in 2019). The highest-profile corporate investigation currently under way started as a result of the criminal proceedings in the *Villarejo* case. José Manuel Villarejo, who has been in custody since late 2017, is a former policeman who allegedly provided intelligence that violated privacy laws or used confidential police information about private clients, including some highly important corporations. The *Villarejo* case is comprised of various judicial proceedings, each focused on the services rendered by Mr Villarejo to one particular client. One single investigating court at the National Court is handling the entire investigation. The different proceedings have evolved separately in each case (in some, the investigating court has dismissed the proceedings while others are still under investigation or even at trial stage).

The case, which is reported widely by Spanish media, has brought the concept and technique of internal investigations to the attention of prosecutors, regulators and even the public.

2 Outline the legal framework for corporate liability in your country.

An amendment to the Spanish Penal Code that introduced corporate criminal liability in Spain entered into force on 23 December 2010. This part of the Penal Code was amended

1 Jaime Alonso Gallo is a partner and Sara Sanz Castillo is a senior associate at Uría Menéndez Abogados, SLP.

© Law Business Research 2021

again in 2015 to include the regulation of effective compliance programmes as a corporate criminal defence.

The corporate criminal liability system in Spain follows neither the vicarious liability model (*respondeat superior*) nor the identification doctrine. The Supreme Court has established that the principle of culpability requires that corporate criminal liability is based on the corporation's own action (Supreme Court Decision (STS) 154/2016). The conduct inherent to the corporation is not the action of its officers or employees, but instead the existence of a flawed organisation (owing to the lack of an adequate preventive system and compliance corporate culture) that made the crime possible. This is the conduct that gives rise to the corporation's liability and, as such, has to be proven by prosecutors.

Corporate criminal liability does not exclude individual liability; on the contrary, corporate liability requires the commission of a crime by the corporation's directors, legal representatives or employees when acting within the scope of the company's activity, on its behalf, and for its direct or indirect benefit. Notwithstanding this, corporations can be held criminally liable, in certain cases, in the absence of an individual's criminal conviction.

The offences for which a legal entity can be held criminally liable are limited to a closed list that includes most criminal offences that are relevant for companies (e.g., corruption, fraud, tax evasion, illegal financing of political parties, illegal trade activities and money laundering).

Aside from criminal liability, corporations can also be subject to penalties for the infringement of administrative regulations applicable to their business activity (e.g., tax legislation, anti-money laundering (AML), countering the financing of terrorism or the stock market). In administrative liability cases, having an effective compliance programme is not an affirmative defence to avoid liability.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The authority to investigate and punish criminal offences is allocated to the regional criminal courts according to the territory where the offence was committed. The National Court has territorial jurisdiction over all of Spain and is entrusted with the investigation and conviction of the most serious cases.

Public prosecutors are in charge of prosecuting criminal wrongdoing and lead the criminal investigation in all the cases that have special relevance, with the aid of specialist bodies within the National Police (e.g., the anti-fraud unit), the Civil Guard (e.g., the Central Operating Unit) and the Tax Agency (e.g., the Customs Surveillance Service). Public prosecutors can also conduct preliminary investigations. Within the Public Prosecutor's Office, specialist divisions are entrusted with the prosecution of specific offences. Chief among them is the Anti-Corruption Public Prosecutor's Office.

The National Public Prosecutor's Office has issued two memoranda on the prosecution of legal entities – Circular 1/2011 and Circular 1/2016 – following the 2010 and 2015 amendments to the Penal Code. These protocols provide an authorised interpretation of the law and give instructions to prosecutors as to its application.

The investigation, prosecution and sanctioning powers in connection with an infringement that is not criminal but regulatory are conferred to distinct administrative authorities,

© Law Business Research 2021

such as the Securities Market National Commission (the stock market regulator), the Bank of Spain, the National Commission for Markets and Competition and the Tax Agency, depending on the nature of the infringed legislation.

There is no evidence of specific authorities refraining from pursuing cases in relation to matters subject to investigation that have been conducted by other authorities.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Criminal complaints can be filed in a criminal court, with the Public Prosecutor's Office or the police. In all cases, the threshold to process a complaint and initiate judicial proceedings is particularly low.

Two peculiarities of the Spanish criminal system increase the prevalence of criminal proceedings: (1) any natural or legal person can file a criminal complaint (even if not the victim of the alleged crime) and become a party to the criminal proceedings; and (2) a civil claim for damages caused by the alleged crime can be filed and adjudicated within the criminal proceedings. Consequently, criminal courts are often used as a channel for litigation between private parties.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

In general, orders and subpoenas issued by a criminal court can be challenged before the same court and a higher court. The grounds for the challenge can vary depending on the case (e.g., a judicial order can be challenged for being over-expansive).

Spanish law does not establish mechanisms to appeal requests issued by public prosecutors when they conduct preliminary investigations.

Decisions issued by prosecutors within a European Investigation Order (Directive 2014/41/EU) cannot be challenged (Article 13.4 of Law 23/2014, which transposes the Directive).

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Except in a few very limited cases (relating to bribery, tax evasion and social security fraud), Spanish legislation does not establish mechanisms similar to leniency agreements. The Penal Code's only prescription in this respect is a reduced penalty for individuals who confess to having committed a crime before the initiation of criminal proceedings (Article 21.4). Notwithstanding this, co-operation between investigated individuals and public prosecutors is common in practice.

7 What are the top priorities for your country's law enforcement authorities?

Prosecutions and convictions for corruption have been highly prominent in Spain, and the focus of prosecutors' investigations and public attention.

© Law Business Research 2021

'Corruption' is a broad concept that includes virtually all crimes committed by public officials (bribery, misuse of public funds, influence peddling, breach of office, etc.).

Prosecution for cybercrime has gained importance during recent months as the authorities are paying greater attention to crimes committed via social networks, cyber-attacks and ransomware.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Compliance programmes were introduced in the Penal Code in 2015. However, their regulation is limited to Article 31 *bis*, which establishes the conditions for compliance programmes to be deemed 'effective', thus being suitable for the exoneration of a corporation.

Following the 2015 amendment to the Penal Code, the National Public Prosecutor's Office issued Circular 1/2016, according to which prosecutors need to verify that a compliance programme 'reflects a corporate commitment that prevents criminal behaviours within the company'. In addition to the requirements set out in Article 31 *bis*, the Circular considered self-reporting and internal investigations to be features typical of effective compliance programmes.

The Supreme Court has enhanced the importance of compliance programmes as a defence mechanism for corporations (e.g., STS 316/2018 of 26 June). Although, case law tends to consider that this defence mechanism should be discussed during the trial stage rather than the investigation stage of judicial proceedings (e.g., Decision 351/2017,of 15 September, of the National Court on the *Bankia* case), there has been case law from the National Court dismissing criminal proceedings already at the investigation stage on the grounds of the existence of an effective compliance programme within the company (e.g., Decision 136/2020, of 7 May, of the National Court on the *Púnica* case).

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

The EU General Data Protection Regulation (GDPR) imposes a general obligation on the data controller and the data processor to implement 'appropriate' measures to protect personal data, as well as the obligation to notify any data breach to the authorities and the concerned data subject. In addition, the Law on Personal Data Protection (Basic Law 3/2018) (LOPDP) sets out a sanction for the infringement of the obligation to secure personal data.

The Spanish Authority for Data Protection (AEPD), in collaboration with the National Institute of Cybersecurity, published Guidelines for the Management and Notification of Security Breaches in 2018.

© Law Business Research 2021

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Penal Code regulates an array of cybercrimes. Those most likely to occur in the context of any business activities include offences against privacy affecting cyberdata or perpetrated by means of information technology (IT) tools (Articles 197 *bis* and 197 *ter*), fraud consisting of making an unauthorised transfer of any asset by means of a computer or IT manipulation (Article 248.2), damaging IT data (Articles 264, 264 *bis* and 264 *ter*), and the unlawful collecting of business information (trade secrets) by using IT instruments (Article 278).

In all these cases, a corporation can be held liable for the commission of the offence, provided that the legal requirements are met (as provided for by Article 31 *bis* of the Spanish Penal Code).

In May 2010, Spain acceded to the Budapest Convention on Cybercrime of the Council of Europe, setting out a guideline for developing legislation to fight cybercrime.

Both the National Police and the Civil Guard have special units dedicated to cybercrime.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Spanish jurisdiction is defined in Article 23 of the Basic Law on the Judiciary (LOPJ). A territorial criterion applies, although there are exceptions to this general rule. One exception is the extraterritorial effect established for offences committed overseas by a Spanish national.

The extraterritorial effect of Spanish criminal law is also set out with regard to specific acts committed abroad, irrespective of the nationality of the perpetrator. Those offences either relate to the protection of fundamental values of the Spanish nation or intend to combat particularly egregious actions (e.g., corruption-related offences committed overseas between private parties or in international business transactions, although, in these cases, additional requirements apply for the prosecution of the misconduct).

The Penal Code establishes additional statutory exceptions to the territorial criterion. For instance, money laundering offences can also be prosecuted by the Spanish authorities even when the offence preceding the money laundering activity was committed overseas or when the activity was totally or partially performed outside the Spanish territory.

Corruption falls within the scope of Spain's jurisdiction regardless of the nationality of the public authority involved in the underlying acts.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The main challenge results from disparities in data protection frameworks, particularly when dealing with countries outside the European Union.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The *non bis in idem* principle is enshrined in the Spanish Constitution, the European Convention on Human Rights and the rules in the Basic Law on the Judiciary (Article 23.2c). This principle also protects legal entities. The Supreme Court has declared (in a ruling of 14 January 2000) that the principle applies both to domestic and international proceedings (although the European Court of Human Rights has not applied it to rulings issued by courts in different countries). Spain has not made any declaration to limit the application of the *non bis in idem* principle in the Schengen area.

Anti-piling on policies, in turn, are not necessary because Spanish law forbids the imposition of a regulatory sanction when misconduct previously resulted in a criminal conviction. To guarantee this, administrative sanction proceedings cannot be conducted while criminal proceedings are continuing.

It is not yet clear whether recent EU case law (i.e., rulings in the *Menci*, *Garlsson Real Estate*, *Di Puma* and *Zecca* cases) will affect Spanish law in the future, other than that, under some conditions, there can be a duplication of 'criminal proceedings/penalties' and 'administrative proceedings/penalties of a criminal nature' against the same person with respect to the same acts.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common in Spain.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Pursuant to the *non bis in idem* principle (which is enshrined in the Spanish Constitution and procedural regulations, as well as in the European Convention on Human Rights), a duplication of criminal proceedings or penalties against the same person with respect to the same acts is prohibited in Spain. Furthermore, the Supreme Court has declared that this principle applies to both domestic and international proceedings. Hence, at least in theory, the existence of a foreign criminal ruling or proceedings on a matter should prevent the Spanish authorities from conducting a new investigation on the same facts against the same individuals.

© Law Business Research 2021

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Spain participates in the mandatory sanctions programmes adopted by the European Union.

Article 42 of the Spanish Anti-Money Laundering Law (Law 10/2010) establishes that financial sanctions adopted by United Nations Resolutions in relation to the prevention and combating of terrorism and the financing of terrorism, and to the prevention, combating and disruption of weapons of mass destruction and the financing thereof, are applicable in Spain with the consequences established by the Spanish government or in EU Regulations.

Aside from sanctions, export controls apply in relation to specific goods (such as double-use technologies).

An infringement of the restrictive measures and export controls regime can constitute a smuggling offence, which could potentially result in criminal liability for a company and the corresponding natural persons (Basic Law 12/95, Article 2) or an administrative offence.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Spanish authorities have not been very active in this area. To date, the Spanish Council of Ministers has not adopted any sanctions in addition to those established by the European Union.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Article 48 *bis* of the Spanish Anti-Money Laundering Law expressly establishes co-operation with other EU Member States for the enforcement of sanctions regulations, among other things. In the case of non-EU countries, co-operation is carried out pursuant to international treaties.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Law 27/1998 of 13 July implemented Council Regulation (EC) No. 2271/96 of 22 November 1996 (the EU Blocking Regulation) in Spain and established economic fines for infringements.

© Law Business Research 2021

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Pursuant to Law 27/1998 of 13 July, the concerned Spanish company must notify the European Commission (within 30 days) of any situation in which its economic or financial interests could be affected by the EU Blocking Regulation and refrain from executing any action against the content of these European provisions.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

In our experience, allegations of misconduct most often come to light through media reports, internal audit, private litigation and regulatory inspections.

As whistleblower protection channels have only been implemented by Spanish corporations to any great extent since 2010 (when corporate criminal liability was introduced in Spanish regulations) and increasingly since the 2015 amendment of the Penal Code, it is too soon to test their effectiveness, as well as the effects that Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law might have.

Tax authorities and other administrative bodies are legally obliged to report to the public prosecutor any potential misconduct identified during their inspection procedures.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The data protection regime consists of Article 18.4 of the Spanish Constitution, the Lisbon Treaty, the EU General Data Protection Regulation (GDPR) and the Law on Personal Data Protection (Basic Law 3/2018) (LOPDP), approved on 5 December to comply with the new EU data protection standards. Corporations are excluded from this protection regime.

Law 34/2002 of 11 July and Law 9/2014 of 9 May regulate data protection in relation to information technology services and e-commerce, and telecommunications, respectively.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The main authority responsible for the enforcement of the data protection regime is the Spanish Authority for Data Protection (AEPD), which can impose fines of up to €20 million or, in the case of corporations, up to 4 per cent of global annual turnover.

Decisions adopted by the AEPD can be challenged in administrative courts.

© Law Business Research 2021

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Although the Spanish regime on data protection does not include any specific provision on internal investigations, this regime must be borne in mind when conducting an investigation of a company.

The processing of data is only legitimate if based on one of the grounds established in Article 6 of the GDPR. In the case of an internal investigation, a corporation can claim the application of Article 6.1.c, which deems the processing of data to be lawful when carried out to comply with a legal obligation to which the controller is subject. This exception would not permit the processing of data based on non-EU regulations, as that is expressly excluded by the AEPD.

The exchange of information with non-EU countries is permitted only to the extent that the non-EU country has in place an equivalent data protection regime. If it does not, the exchange can be carried out only in the exceptional cases established in Article 49 of the GDPR. As Article 49.1.e permits the transfer of personal data when necessary for the establishment, exercise or defence of legal claims, this provision could be claimed to permit the transfer of data to a non-EU country. However, the validity of this argument must be assessed in each case.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Spain restricts the interception of employees' communications, both through the interpretation and application of workers' rights by courts and through statutory provisions in data protection law.

As to case law, labour courts have adopted a set of standards that are similar to those established by the European Court of Human Rights in the *Barbulescu II* ruling (Grand Chamber, *Barbulescu v. Romania*, 5 September 2017) and are also followed by the AEPD and by criminal courts (e.g., Supreme Court Decision (STS) 489/2018 of 23 October and STS 328/2021 of 22 April). According to these standards, (1) the employer must have informed employees of the possibility of their correspondence being monitored (normally through a written policy), with the result of limiting the expectation of privacy in the use of corporate email, and (2) accessing an employee's email must be grounded on a legitimate aim and comply with the proportionality test.

As to statutory restrictions, the LOPDP includes a number of 'digital rights', among them the 'right to privacy in the use of digital devices in the workplace' (Article 87). Pursuant to this Article, employers are permitted to access the contents of the digital devices provided by the company to employees only if that access is for the sole purpose of controlling the observance of labour or statutory duties or guaranteeing the devices' integrity. Employers must establish criteria for the use of digital devices (and inform employees about them), which must guarantee the minimum standards of privacy protection according to social customs and constitutional rights.

Provided that the standards described above are met, the consent of employees is not necessary to conduct the monitoring, although consent could act as an additional

© Law Business Research 2021

guarantee for the employer to prove the lawfulness of reviewing emails. Notwithstanding this, the validity of consent has been limited in some fields (in particular, in the context of data protection).

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants are common in corruption cases. In other white-collar cases, the use of judicial production orders is more common.

The Criminal Procedure Law (LECr) and its interpretation by the Supreme Court establishes legal limits on raids and, since 2015, a specific regulatory framework applies to searches and seizures of computers, devices for telephonic or electronic communication, devices for mass storage of information and electronic data repositories (Articles 588 *bis* to 588 *septies*).

The investigating judge's ruling can be challenged before the same court and a higher court. Evidence obtained in breach of the legal limits can be suppressed from the trial.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

In practice, the exclusion of privileged material does not usually occur during a dawn raid, but rather at a second stage, when the contents of the seized devices are transferred to the judicial records. Nevertheless, it is advisable to warn the court clerk and the police during a search of the existence of privileged material and to include that warning in the minutes of the search written by the court clerk and signed by the representative of the searched corporation.

Material that is unnecessary for the investigation and affects the privacy of the defendant or third parties is normally suppressed (Basic Law on the Judiciary, Article 236 *quinquies* and LECr, Article 586 *ter* i). This mechanism can also be used to suppress privileged material. Furthermore, Article 118.4 of the LECr expressly establishes the confidentiality of communications between a defendant and his or her lawyer and their suppression from the judicial file, except in the event of indicia of the lawyer's co-operation in the commission of the criminal action.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The Spanish Constitution guarantees the right against self-incrimination (Article 24.2). This right also protects legal entities (LECr, Articles 409 *bis* and 786 *bis*).

© Law Business Research 2021

Defendants in criminal proceedings have the right to testify in court, both during the investigation stage and at the trial. When exercising this right, defendants have no obligation to tell the truth and cannot be convicted of perjury.

Witnesses are obliged to appear in court, give testimony and tell the truth (LECr, Article 410), with a few exceptions (LECr, Article 416). A witness's failure to appear before a court can lead to the imposition of a fine and, under certain circumstances, a conviction for either obstructing justice or severe disobedience.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The regulation of compliance programmes in the Penal Code has been interpreted in a manner that has made whistleblower protection channels compulsory in order for a company to be entitled to benefit from this defence (e.g., the National Public Prosecutor's Office's Circular 1/2016).

No financial incentives are established for individuals who report misconduct. Taking into account the Supreme Court's doctrine on evidence, this practice would severely limit whistleblowers' credibility as witnesses.

Labour law protects whistleblowers from both unfair dismissal and unfair treatment by the company resulting from an internal complaint.

Regarding anonymous reporting, this is allowed under the Law on Personal Data Protection (Basic Law 3/2018) and the Anti-Money Laundering Law. The Criminal Section of the Supreme Court has accepted anonymous corporate reporting as a valid means to trigger an internal investigation and follow-up criminal proceedings (Ruling 35/2020 of 6 February).

Directive (EU) 2019/1937 has not yet been transposed into Spanish legislation but, at the time of writing, the process is under way.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Spanish labour law vigorously protects workers from unfair treatment or dismissal. This protection also extends to the context of an investigation. Furthermore, there is a general consensus that investigated individuals should enjoy the right to defence in internal investigations.

© Law Business Research 2021

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Article 31 *bis* of the Penal Code establishes that one requirement for an effective compliance programme is a disciplinary system that adequately punishes failures to comply with the programme's measures.

As to labour law, an employer is entitled to sanction (including through dismissal) employees who have been involved in misconduct within the scope of their professional activities. The sanction would be grounded on the infringement of the principle of good faith that governs labour relations.

In the event that an employee is suspected of having been involved in wrongdoing, the employer would generally be entitled to arrange the suspension of the employee's activities within the company (although the specific circumstances should be taken into consideration).

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Labour law allows employers to give instructions to employees, including instructions for an employee to provide information about his or her actions within the company.

A lack of co-operation could lead to the imposition of disciplinary measures against an employee, although multiple factors would have to be analysed, the most important being the employee's obligation to co-operate in internal investigations – or similar procedures – in the employment contract or the company's internal regulations. Other factors to take into consideration include the severity of the disobedience and the employee's position within the company. Labour courts tend to be highly protective of employees in conflicts with employers.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Terms of references have become more common in Spain recently, although there is still no standard practice in this regard.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Article 31 *bis* of the Penal Code requires that the supervision of the programme be entrusted to a body within the legal entity with autonomy and independence and that

© Law Business Research 2021

the body should be informed of any issue that comes to light. Large Spanish companies normally have a protocol detailing what should be done if wrongdoing or any breach of internal rules is detected.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

If an order suggests that a corporation may be under investigation or that any of its employees, officers or directors may have engaged in illegal acts, the best practices in compliance suggest that the corporation should attempt to investigate the facts. Further, recent practice shows that the authorities would expect the company to conduct an internal investigation.

Nevertheless, legal persons are protected by the right against self-incrimination. This constitutional guarantee is normally interpreted as implying that corporations cannot be obliged to produce documents that may incriminate them (but obviously may be subject to search warrants).

Article 588 *octies* of the Criminal Procedure Law establishes that the Public Prosecutor's Office or the police can issue an order for the preservation of data or information stored in computer systems for up to 90 days to allow a judicial order to be issued during that time.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Corporations are obliged to publish specific non-financial information, including the main risks associated with anti-bribery matters (Commercial Code, Article 49.6). An internal investigation or contact from a law enforcement authority about corruption may trigger this disclosure obligation.

Listed companies are obliged to publish an annual corporate governance report (Corporations Law, Articles 538 and 540). The corporate governance report must include information about the main risks that can affect the achievement of business objectives and the risks that have materialised during the year (Circular 5/2013 of the Securities Market National Commission (CNMV)).

This information must also be included in any prospectus of securities issues.

Finally, if information about an internal investigation, were it to be made public, is likely to have a significant effect on the prices of the financial instruments issued by the company in question (or on the price of related derivative financial instruments), the company will be subject to the rules on the disclosure of inside information established in Regulation (EU) 596/2014 on market abuse (Article 17) and to disclosure obligations under the Securities Markets Law (Articles 225 to 229).

A public notice issued by the CNMV reminds listed companies of their obligation to comply with these obligations when they may be involved in allegedly irregular practices, remarking that information regarding these risks disclosed by issuers should be sufficiently detailed to allow the market and investors to comprehend the significance and relevance of the facts and risks.

© Law Business Research 2021

37 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are increasingly encouraged by the National Public Prosecutor's Office (according to Circular 1/2016, providing that evidence to law enforcement authorities obtained during an internal investigation will be regarded by prosecutors as proof of the corporation's ethical commitment and, as such, may lead to exoneration of criminal responsibility) and by the CNMV (in its proposal of 14 January 2020 of an amendment to the Code of good practices for corporations).

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

According to the Basic Law on the Judiciary (Article 542.3) and the new Lawyers' General Statute (Article 22.1), privilege protects all facts or information known by lawyers as a result of their professional activity.

This definition of privilege is particularly broad. The Lawyers' Deontological Code includes within the scope of privilege (1) any confidential information or proposal received by a lawyer from his or her client, from a counterparty and from other colleagues, (2) any documents sent or received by a lawyer as a result of any of the forms of his or her professional activities, and (3) any communications exchanged between lawyers, including negotiations, whether oral or written.

The Deontological Code is not positive law but rather a professional code of conduct that binds lawyers to a set of ethical standards that courts may or may not apply in their interpretation of the law.

There has been a tendency in case law to try to limit the scope of privilege protection to that accepted in the regulation of anti-money laundering (AML) and countering the financing of terrorism. As from the Second AML Directive (Directive 2001/97/EC), the European Union has established that lawyers are obliged to report suspicions of money laundering unless they are ascertaining the legal position of a client or representing a client in legal proceedings (or in relation to legal proceedings, including legal advice on the initiation or avoidance of legal proceedings, see Article 22 of the Anti-Money Laundering Law).

There is no specific regulation on how privilege operates in the context of internal investigations, although there are no legal grounds to conclude that these same contents should not be protected by privilege. Indeed, an internal investigation is a technique to ascertain the legal position of the client and to defend the client in legal proceedings (criminal or regulatory), whether actual or potential.

It is customary to attempt to protect confidentiality through external counsel, but it is not clear to what extent external lawyers' intervention guarantees privilege.

© Law Business Research 2021

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Privilege (or professional secrecy) is conceived as both a right and a professional duty of lawyers, legally protected to guarantee the client's right of defence.

The lawyer is entitled to claim privilege to avoid disclosing documents or communications relating to his or her professional activities and to refuse to act as a witness in a judicial case when that testimony refers to the lawyer's activities as legal counsel.

None of the legal provisions on privilege makes any distinction between clients who are legal or natural persons.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

According to resolutions issued by the European Court of Justice, in-house lawyers are not holders of legal privilege (Ruling in Case C-550/07 P, *Akcros Chemicals Ltd v. the European Commission*). However, to date, this restrictive interpretation of attorney–client privilege has only been established in competition law cases, and it is unclear whether it will be extended to other areas. Regarding domestic regulations, the new Lawyers' General Statute (approved by Law 135/2021 of 2 March and in force since 1 July 2021) expressly includes legal privilege as one of the principles applicable to in-house lawyers. There is no specific and clear Spanish case law in this regard.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Regulations do not distinguish between Spanish and foreign lawyers. In practice, it is understood that the attorney–client privilege also applies to communications with foreign lawyers.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The concept of waiver of the attorney–client privilege has not been developed in Spain. In fact, the client's sole consent to the disclosure of information or documents does not release the lawyer from the obligation of professional secrecy (Deontological Code, Article 5.8).

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

This concept has not yet been recognised in Spain.

© Law Business Research 2021

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This concept has not yet been recognised in Spain.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept itself is not recognised in Spain. However, attorneys advising multiple parties are entitled to share communications and documents, which are in turn subject to privilege. Common interest agreements are used in internal investigations.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Recent judicial cases show that it is not yet clear to what extent external lawyers' intervention guarantees confidentiality. Best practices suggest involving an external lawyer in the engagement of any third party (e.g., a forensic firm) and in any communication and production of documents process.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

No statutory provision refers to this possibility. In practice, it is common to interview witnesses as part of an internal investigation.

The evidentiary value of interviews in criminal proceedings may be limited, especially if the interviewee is not assisted by a lawyer.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Since the interviewee is not the client, it is doubtful that interviews are protected by privilege, considering the general rules applicable on legal privilege (i.e., Basic Law on the Judiciary, Article 542.3; new Lawyers' General Statute, Article 22.1; Lawyers' Deontological Code, Article 5).

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Interviews in an internal investigation can be conducted in different ways depending on their purpose. There is no specific regulation or general standard concerning the requirements to be met when conducting interviews.

In practice, it is common to issue warnings similar to those established in other jurisdictions (e.g., to inform the interviewee that he or she has the right to be assisted by a lawyer).

© Law Business Research 2021

Further, *Upjohn* warnings are usually issued at the beginning of interviews as an ethical (and preventive) measure to avoid potential confusion about the interviewer's role and legal duties.

The requirements do not differ when interviewing third parties.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

If any documents are produced, this is usually done during an interview as a means to seek an employee's assistance in an investigation.

The attendance of a lawyer assisting the employee is not a compulsory requirement in Spain, although it may in some circumstances be a good option (e.g., to strengthen the evidentiary value of the interview in subsequent criminal proceedings).

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Articles 259 and 262 of the Criminal Procedure Law impose a general obligation on any individual who witnesses an offence (or knows of the existence of an offence through his or her professional activity) to report misconduct. However, the consequences set out for the infringement of this obligation are purely symbolic (a maximum fine of less than €2) and the obligation is never enforced in practice. Only civil servants have an actual obligation to report misconduct of which they become aware in the course of their professional activities. If they fail to do so, they may be held criminally liable and face a penalty of professional debarment.

However, reporting misconduct is mandatory pursuant to anti-money laundering and countering the financing of terrorism (Anti-Money Laundering Law, Article 63 read with Article 18) and market abuse regulations (Regulation (EU) No. 596/2014, Article 16.2).

An obligation to self-report does not exist for either legal or natural persons as a result of the right against self-incrimination granted by Article 24.2 of the Spanish Constitution.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The Penal Code considers self-reporting a mitigating circumstance for both legal and natural persons. In addition, according to the National Public Prosecutor's Office Circular 1/2016, prosecutors are instructed to request exoneration of criminal responsibility for the corporation that self-reports a criminal offence.

However, public prosecutors are not the only accusing parties – a feature that adds an additional element of complexity to settlements, compared with other jurisdictions.

Regulators increasingly expect corporations to act transparently and co-operatively when allegations of criminal conduct are known.

© Law Business Research 2021

Taking into consideration all these factors, self-reporting and co-operation are highly recommended in serious criminal cases. If the alleged criminal conduct has multi-jurisdictional implications, this advice may extend to other countries, although this possibility depends on the characteristics of the legal system and law enforcement in those countries.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

The general way to self-report is to conduct the necessary meetings to explain the facts to prosecutors and to file the complaint with them, initiating the necessary co-operation and negotiation.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is generally advisable that companies seek external legal counsel to respond to a notice or subpoena, even when the corporation is not yet formally an investigated party.

It is possible to approach the prosecutor or the investigating judge to discuss the deadline for the request or understand its scope.

55 Are ongoing authority investigations subject to challenge before the courts?

Authority investigations in Spain take place within the context of criminal proceedings conducted by a criminal court. The decisions adopted by the court as part of the investigation can generally be challenged before that court and a higher court.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The best way to answer separate requests can only be assessed in each particular case. Nevertheless, assuming that co-operation between different countries' authorities is highly probable, the best approach probably consists of three elements: (1) informing each authority of the requests made by the other country's authority; (2) attempting to limit the scope of each request to what is relevant and legally admissible in each country; and (3) ensuring consistency in the answers to the different requests.

© Law Business Research 2021

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If the authorities' capacity to investigate and prosecute an extraterritorial matter is well established in Spanish law (as in cases of foreign corruption), the company must comply with the request, searching documents and data and producing them in the proceedings (with a caveat regarding the right against self-incrimination). Complications will arise if there are any legal restrictions in the country of origin of the evidence.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Co-operation between Spanish and foreign authorities is increasingly common and enhanced by different mechanisms:

- the mutual recognition system within the EU criminal justice system;
- mutual legal assistance treaties;
- exchange of information in the application of the Organisation for Economic Co-operation and Development's Common Reporting Standard;
- exchange of information in the application of double taxation treaties; and
- co-operation agreements between regulators of multiple countries.

Spanish statutes on specific activities expressly regulate international co-operation (e.g., Article 61 of Law 10/2014 for banking supervision authorities, Articles 244 to 247 of the Securities Market Law for co-operation between securities regulators and Article 48 *bis* of the Anti-Money Laundering Law for co-operation between anti-money laundering and counter terrorism financing authorities).

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Regulators (such as the Securities Market National Commission (the stock market regulator), the Bank of Spain and the Commission for the Prevention of Money Laundering and Monetary Offences) normally have confidentiality obligations, as established in their own statutes. These confidentiality obligations cannot restrict the authority of criminal law enforcement authorities (normally, investigating judges) to request whatever information or documentation they consider necessary.

As regards criminal investigations, the investigation stage is confidential (Criminal Procedure Law, Article 301) and only the parties to the proceedings have access to judicial records. However, leaks to the media are extremely common in Spain.

© Law Business Research 2021

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

As a general rule, a company must refrain from producing for Spanish authorities any documents from other countries when production would violate local law. Instead, the conflict should be explained to the authorities and alternative ways to gather the information must be considered. Spanish authorities will normally understand this limitation, as territorial overreach is unusual in practice.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

There are no blocking statutes in Spanish law, except in connection with EU trade sanctions, as Spain participates in the mandatory sanctions programmes adopted by the European Union.

There are secrecy obligations for some types of information, such as for banking records (Law 10/2014, Article 83) and personal data (Law on Personal Data Protection (Basic Law 3/2018) (LOPDP), Article 5), that may restrict voluntary production. This hurdle is normally avoided by submitting a request to the authorities, within the framework of co-operation, for a production order issued by an investigating judge.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

With the exception regarding secrecy obligations (e.g., banking records, pursuant to Law 10/2014, Article 83, and personal data, pursuant to LOPDP, Article 5), the risks of voluntary production and compelled production of material are similar. In both cases, the material produced may be discoverable by third parties (normally through a judicial production order). Confidentiality protection, if any exists, does not differ if production is voluntary or compelled.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Corporations can be subject to a wide range of penalties, including fines, dissolution of the legal entity, suspension of the business activity, closing of premises, debarment from the corresponding business activity, exclusion from public subsidies and public contracts, and judicial monitoring of the company to safeguard employees' or creditors' rights (Penal Code, Article 33.7). Only fines are compulsory in the event of conviction; other penalties are not, and have not been imposed by courts to date. Disgorgement of profits is increasingly significant but is not considered a penalty.

© Law Business Research 2021

Regarding directors, officers and employees, a criminal conviction can result in imprisonment or a fine (or both).

In addition to criminal penalties, the civil liability of the individual and the corporation can be ruled on within the criminal proceedings.

In addition to the penalties established in the Penal Code, the Public Contracts Law (Law 9/2017) establishes a prohibition against entering into public contracts for individuals and corporations who have been convicted for, among other offences, bribery, tax evasion, money laundering, offences against the environment and offences against labour rights, for a maximum of five years (Articles 71 and 72). This prohibition results from the transposition of the EU Public Procurement Directive (Directive 2014/24/EU). However, the transposition of the Directive into Spanish law has been rather restrictive given that, contrary to the Directive, it has excluded compliance programmes as a way to avoid the application of a prohibition when it derives from a criminal conviction.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

A settlement in another country, if it leads to a conviction, may have adverse effects on proceedings in Spain and could trigger exclusion from public procurement.

65 What do the authorities in your country take into account when fixing penalties?

Courts will take into account the severity of the facts and the potential existence of the aggravating and mitigating circumstances laid out in the Penal Code. In the case of corporations, mitigating circumstances include self-reporting of the offence to the authorities, co-operation with the authorities' investigation, implementation of remediation measures and adoption of compliance measures to detect potential future offences (Penal Code, Article 31 *quater*).

The Penal Code does not establish general aggravating circumstances applicable to any corporate offence. However, for some offences, the specific circumstances of the case can lead to a more severe penalty (e.g., when the damage resulting from the offence exceeds a specific threshold).

Further statutory criteria to determine the appropriate penalty within the range established by application of the aggravating and mitigating factors apply with regard to corporations. To that end, among other criteria, courts must take into account the need to impose the penalty to deter future offences within the corporation, the possible consequences that the penalty imposed on the legal entity might have on its employees and the position within the company of the individual or body that failed to comply with the control duties to prevent the wrongdoing (Penal Code, Article 66 *bis*).

© Law Business Research 2021

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Spanish regulations do not establish any legal instruments similar to deferred prosecution agreements (DPAs) or non-prosecution agreements (NPAs).

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

As there are no DPAs or NPAs, there is no regulation on reporting restrictions or anonymity. Any settlement that a company may reach within the context of criminal proceedings will involve an admission of guilt and thus be reflected in a court's ruling, which will form part of the public record. The names of individuals are redacted from courts' decisions and rulings, because of data protection, but not the names of corporations. If there is a public interest in the case, the ruling will normally be available on the internet without any redaction.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

No settlement is possible without an admission of guilt. However, even under these circumstances, a corporation may potentially be interested in reaching a settlement to benefit from a reduced penalty and to be able to negotiate the specific type of penalty to be imposed.

If an offence has resulted in damage to third parties (either authorities, such as the tax authority, or private parties), it is advisable that those parties be involved in the negotiation process. If they are not, the affected third parties could bring (or continue to pursue) criminal actions against the corporation irrespective of the settlement reached with the public prosecutor.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Monitorships are one potential penalty for corporations convicted of a criminal offence (Penal Code, Article 33.7.g), although with a very limited scope (to safeguard employees' and creditors' rights after an offence has been committed). To date, no monitorship has been imposed on any corporation.

© Law Business Research 2021

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Any natural or legal person in Spain can file a criminal complaint (even if not the victim of the alleged crime) and become a party to the criminal proceedings (thus gaining access to the authorities' files).

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

During a judicial investigation, only the parties to the proceedings are entitled to access the judicial file. However, leaks to the media are endemic.

Trials are public and, in high-profile cases, are broadcast live on the internet.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Large corporations tend to have an internal department in charge of the company's communication strategy. In situations of corporate crises, corporations may also seek external specialist support from public relations firms.

73 How is publicity managed when there are ongoing related proceedings?

Any communication should be reviewed by the public relations team and by the legal team to avoid the communication affecting the proceedings or clashing with the company's defence strategy in a judicial case.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

The existence of this obligation has to be analysed in light of commercial and corporate regulations, which oblige corporations to publish specific non-financial information (i.e., Commercial Code, Article 49.6 and, for the particular case of listed companies, Corporations Law, Articles 538 and 540).

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Environmental matters are regulated by a wide array of national, regional and local laws that are constantly changing. Social matters (e.g., gender equality in corporate decision-making bodies) tend to be regulated by centralised initiatives.

Corporate governance is mainly regulated by means of the Commercial Code and the Corporations Law. In addition to these, listed companies are subject to the Securities

© Law Business Research 2021

Market Law, the Code of good practices for corporations and the instructions issued by the Securities Market National Commission (the stock market regulator).

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

No key regulatory changes are expected.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

Any natural or legal person can file a criminal complaint (even if not the victim of the alleged crime) and become a party to criminal proceedings. For this reason, associations tend to be very active on ESG-related matters and, in particular, in the prosecution of environmental offences. However, there has not been a particular increase in this regard in recent years.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The legislative process to draft and pass a new Criminal Procedure Law was initiated in 2021. This potential new regulation could have a tremendous effect on criminal proceedings, as well as on the defence of corporations (e.g., the investigation stage could be handed to the Public Prosecutor's Office instead of investigating courts, as is now the case). However, the draft is still under discussion and it is too soon to assess its potential consequences. In addition, this draft establishes a *vacatio legis* period of six years, thus postponing considerably the entering into force of the potential new regulation.

Furthermore, the outcome of internal investigations has started to be used by companies for their defence in criminal proceedings. Therefore, in the coming years, we will get to see public prosecutors' and courts' reactions to internal investigations (e.g., whether, and under what circumstances, they acknowledge their content as valid evidence).

Finally, it will be interesting to see how case law develops regarding the role of compliance programmes as the grounds for dismissal or acquittal of corporations, and whether the judicial decisions support recent precedents dismissing criminal proceedings already at the investigation stage on the grounds of the existence of an effective compliance programme within a company.

© Law Business Research 2021

23

Switzerland

Flavio Romerio, Claudio Bazzani, Katrin Ivell and Reto Ferrari-Visca[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

In the past few years, Switzerland has been confronted with several multi-jurisdictional investigations relating to corruption, fraud, money laundering and tax evasion. Most of these cases have attracted considerable media attention.

In 2008, the US authorities, and later the Swiss Financial Market Supervisory Authority (FINMA), initiated investigations against several Swiss banks in connection with their US cross-border business. By the end of 2018, more than 90 Swiss banks had reached an agreement with the US authorities and paid penalties totalling more than 6 billion Swiss francs.

Notable also are the investigations launched by FINMA and the Office of the Attorney General (OAG) in connection with the global money-laundering scandal around the Malaysian sovereign wealth fund 1MDB, and the investigations around the FIFA corruption scandal and the diesel emissions fraud scandal.

In connection with Brazil's biggest corruption case – *Odebrecht/Petrobras* (*Operation Car Wash*) – the Swiss prosecutors and FINMA have sent disclosure orders to more than 40 Swiss banks and seized assets valued at more than US$1 billion. By the end of 2018, the Swiss authorities were able to transfer more than 300 million Swiss francs to the Brazilian authorities. In 2018, the OAG initiated criminal proceedings against two Swiss banks.

At the national level, notable cases are the investigations in connection with possible irregularities regarding certain private and business dealings of the former chief executive

1 Flavio Romerio, Claudio Bazzani and Katrin Ivell are partners and Reto Ferrari-Visca is an associate at Homburger.

© Law Business Research 2021

officer of Raiffeisen Bank and the investigation regarding incorrect accounting practices by the state-owned post bus company that had led to receipt of considerably higher subsidies than would otherwise have been due to it. More recently, in a matter that attracted considerable media attention, one of Switzerland's major banks investigated allegations about the surveillance of a former top executive at the bank, and the University Hospital Zurich conducted an investigation into allegations of conflicts of interests of the head of the department of cardiac surgery regarding the use of devices from companies in which he had a stake.

2 Outline the legal framework for corporate liability in your country.

Corporate criminal liability in Switzerland can arise in two situations:

- if it is not possible to attribute an offence to any specific individual because of the inadequate organisation of the corporation; or
- if it fails to take all necessary and reasonable organisational measures to prevent certain offences, such as bribery, corruption, financing of terrorism or money laundering.

The penalty in either case is a fine of up to 5 million Swiss francs.

Corporations may also be fined in administrative criminal proceedings instead of the responsible individual if a penalty of no more than 5,000 Swiss francs will be imposed and the investigations would be disproportionate compared to the fine. If the matter concerns a violation of financial market laws, the fine may be as high as 50,000 Swiss francs.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

There are no specific law enforcement authorities regulating corporations. Accordingly, there are no specific policies or protocols relating to the prosecution of corporations.

At cantonal level, criminal laws are enforced by the regional and cantonal prosecutors with the assistance of the police. Some cantons have specialist prosecutors' offices to deal with business crimes.

At federal level, the OAG is responsible for prosecuting offences that are subject to federal jurisdiction (e.g., espionage, certain cases of corruption, international organised crime and certain white-collar crimes). The Federal Department of Finance is generally responsible for prosecuting offences against financial market laws (e.g., violation of duty to file a suspicious activity report or violation of disclosure rules).

In addition, government agencies enforce administrative laws and regulations. Important regulatory authorities at the national level are FINMA, which is responsible for monitoring financial institutions and enforcing the financial market legislation, and the Competition Commission (COMCO), which is responsible for monitoring companies for signs of anticompetitive conduct, combating harmful cartels and enforcing merger control legislation.

© Law Business Research 2021

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The police, the prosecutors and the Federal Department of Finance are required to open an investigation once they become aware of a potential criminal offence.

FINMA will initiate an investigation if it has reason to believe that financial market laws and regulations have been violated. However, it has some discretion in deciding whether to open formal enforcement proceedings. For example, it may refrain from opening formal enforcement proceedings if a supervised entity fully co-operates and instantly implements all necessary remedial measures to ensure compliance with financial market legislation.

COMCO has adopted guidelines to establish the circumstances under which it will investigate antitrust violations. It usually opens an investigation when an alleged violation is serious or has a significant effect on the market, or when the case raises a legal question that warrants judicial clarification. COMCO usually declines to investigate complaints when the issue could be better solved through private litigation. It can also decline to investigate a complaint when the target business has already changed its policy, or when the target business agrees to adapt its market behaviour or contracts.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

In general, any orders from authorities can be challenged before the competent authorities and courts.

In criminal proceedings (including administrative criminal proceedings), records and objects must be sealed if the owner claims that they may not be searched or seized (e.g., owing to the attorney–client privilege). The authorities then have the possibility to file a request for the removal of the seal before the competent courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Confessions and co-operation during the investigations in administrative criminal proceedings and in criminal proceedings may lead to a reduction in the sentence. However, there are currently no specific immunity or leniency rules in Swiss criminal laws for co-operation. Therefore, an individual must carefully assess the potential benefits and disadvantages and decide in each case whether he or she wants to co-operate with the authorities.

In enforcement proceedings, supervised entities and individuals are in general required to provide all information and documents that FINMA requests to fulfil its supervisory tasks. In this context, co-operation is not a mitigating factor but a statutory obligation. However, a supervised entity or an individual is going to be more able to negotiate an alternative resolution and to avoid formal enforcement proceedings if it agrees to co-operate with FINMA and take remedial measures.

COMCO has adopted a leniency policy that closely mirrors the model of the European Commission's programme. Companies may be granted complete or partial immunity

© Law Business Research 2021

from sanctions if they self-report, hand over all available evidence and fully co-operate with COMCO. However, only the company that first reports a cartel may benefit from full immunity. Companies reporting subsequently may receive a reduction of their fine if they provide significant additional evidence.

In tax law, voluntary disclosure may lead to a mitigation or waiver of punishment if certain requirements are met.

7 What are the top priorities for your country's law enforcement authorities?

In recent years, the focus of the Swiss law enforcement authorities has been on corruption, fraud and money laundering cases. In addition, there has been an increase in criminal proceedings in connection with cybercrime.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

There is no universal legal requirement under Swiss law to have an effective compliance programme. However, failure to have an effective compliance programme may lead to corporate criminal liability (i.e., a fine of up to 5 million Swiss francs).

For some industry sectors (notably banking and insurance), there are rules requiring effective compliance processes and control functions. The requirements are listed in two circulars regarding corporate governance published by FINMA.

The State Secretariat for Economic Affairs (SECO) has published best practices for an Internal Control Programme for Export Controls (ICP) and a fact sheet for the ICP, as well as a guide to companies operating outside Switzerland on how to fight and prevent corruption. The latter contains high-level guidance on what an anti-corruption code of conduct should contain. It also refers to additional literature and guidance issued by, among others, Transparency International or the International Chamber of Commerce.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Currently, there is no specific legislation regarding cybersecurity. Instead, cybersecurity is regulated by a variety of Swiss laws and regulations.

Pursuant to the Federal Data Protection Act, personal data must be protected against unauthorised processing through adequate technical and organisational measures. In general, any violations of this principle must be enforced by bringing an action before the civil courts. The Federal Data Protection and Information Commissioner has currently no enforcement powers.

© Law Business Research 2021

Based on the Financial Market Infrastructure Act, financial market infrastructures are required to operate information technology systems that ensure the availability, confidentiality and integrity of data relating to participants and their transactions. Violations of these requirements might lead to investigations or, in serious cases, to formal enforcement proceedings by the Swiss Financial Market Supervisory Authority (FINMA). Data breaches concerning data covered by Swiss bank secrecy may result in imprisonment for up to three years or a monetary penalty of up to 540,000 Swiss francs.

Currently, there is no general statutory duty to report data breaches. Depending on the circumstances, however, it might be advisable to notify the data subjects affected by a breach based on the general data processing rules. In addition, there are some sector-specific reporting obligations, including in the financial services, telecommunications, aviation, railway and nuclear sectors.

It is also possible (not an obligation) to inform the Swiss Reporting and Analysis Centre for Information Assurance (known as MELANI) about cyber incidents.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

There is no specific law in Switzerland that regulates cybercrime. However, there are several provisions in the Swiss Criminal Code that are specific to cybercrime, including unauthorised obtaining of data or unauthorised access to a data processing system. Depending on the circumstances, other criminal provisions may be applicable also, such as document forgery, extortion, coercion and money laundering.

Switzerland is a member of the Budapest Convention on Cybercrime. The main objective of the Convention is to pursue a common criminal policy aimed at protecting society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Generally, the Swiss authorities have jurisdiction over offences committed in Switzerland. An offence is deemed to have been committed in Switzerland if the accused person acted in Switzerland or the offence had effects in Switzerland.

In specific cases, Swiss courts also have jurisdiction over offences committed abroad, including:

- offences against the Swiss state or its national security;
- specific offences against minors (e.g., trafficking, sexual assault, rape);
- offences that Switzerland undertook to pursue based on an international treaty if the offence is also punishable in the place abroad where it was committed; and
- offences that are punishable both in Switzerland and the place abroad where they were committed if the offence in question is an extraditable offence and the accused person is located in Switzerland but not extradited.

© Law Business Research 2021

If the offence was committed abroad, the main evidence often needs to be obtained through international mutual legal assistance, which might be a lengthy process depending on the foreign authorities involved. Swiss authorities are thus usually selective in the prosecution of such offences. Instead, they try to prosecute foreign offences indirectly by targeting the accused persons for related offences committed in Switzerland (in particular, money laundering).

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The typical issue in cross-border investigations is the transfer of personal data from Switzerland to foreign courts, regulators or enforcement authorities. Several legal provisions restrict the disclosure of personal data to foreign authorities, inter alia, the prohibition of unlawful activities on behalf of a foreign state (Swiss Criminal Code, Article 271), Swiss banking secrecy (Federal Banking Act, Article 47), Swiss data protection and labour laws. Additionally, contractual secrecy obligations or confidentiality agreements may prevent the disclosure of data.

Article 271 of the Criminal Code prohibits and sanctions activities on behalf of a foreign state on Swiss territory unless the competent administrative body has granted an authorisation. In general, Switzerland-based corporations and individuals are thus required to obtain authorisation if they intend to disclose personal data to foreign authorities.

Pursuant to Article 47 of the Federal Banking Act, it is an offence to disclose confidential information about current or former clients of a Swiss bank. A breach of Swiss banking secrecy may not only trigger criminal sanctions but also administrative measures or proceedings and civil liability.

The Federal Data Protection Act requires, inter alia, that personal data only be processed in compliance with specific processing rules (e.g., rules of lawfulness, good faith, proportionality and transparency). In addition, Article 6 of the Act provides that personal data may not be disclosed to recipients outside Switzerland if this seriously endangers the privacy of the data subject. Such a risk is presumed a matter of statutory law if the country of destination is lacking adequate data protection regulation. The Federal Data Protection and Information Commissioner maintains a list of countries that are deemed to have adequate data protection.

When foreign authorities use the available channels of mutual administrative or legal assistance to obtain documents and information, the aforementioned provisions do not apply.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Switzerland applies the *ne bis in idem* doctrine, which is essentially the equivalent of the double jeopardy concept in common law jurisdictions. Based on this doctrine, no person who has been convicted or acquitted in Switzerland in a final legally binding judgment may be prosecuted again for the same offence. This also applies to corporations. Owing to the territoriality principle, a foreign prosecution or conviction has, in general, no effect on the jurisdiction of Swiss criminal authorities regarding offences committed in Switzerland. Under certain conditions, however, the Swiss criminal authorities have to observe a foreign verdict of acquittal or reduce a sentence if it has already been partly served abroad.

If an investigation pursues the same subject matter, multiple government authorities may simultaneously investigate the same corporation. If appropriate, they usually coordinate their actions and may consult each other to ensure that their investigations do not interfere with each other or duplicate the same enquiries. The *ne bis in idem* doctrine prohibits multiple Swiss authorities from penalising companies for the same conduct. However, in general, the doctrine has no effect on civil or regulatory proceedings. Therefore, regulatory authorities may order additional measures against a corporation even if that corporation has already been convicted or acquitted in criminal proceedings.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not frequent in Switzerland. However, the Swiss authorities do co-operate with foreign authorities based on applicable laws, in particular in connection with multi-jurisdictional investigations.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

In general, Swiss authorities conduct their investigations independently. However, investigations or decisions of foreign authorities may cause the Swiss authorities to initiate an investigation.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Switzerland's sanctions programme authorises the Federal Council to impose non-military measures to implement sanctions that have been imposed by the United Nations, the

© Law Business Research 2021

Organisation for Economic Co-operation and Development or by Switzerland's most significant trading partners (e.g., the European Union) for the enforcement of international law, in particular of human rights.

Possible sanctions are direct or indirect restrictions on transactions involving goods and services, payment and capital transfers; the movement of persons; scientific, technological and cultural exchange; prohibitions; licensing and reporting obligations; and other restrictions of rights.

In general, Switzerland updates its sanctions lists in accordance with those issued by the United Nations.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The State Secretariat for Economic Affairs (SECO) is the main authority with responsibility for monitoring and implementing sanctions. A breach of sanctions may result in imprisonment for up to five years, which may be combined with a fine of up to 1 million Swiss francs.

SECO does not publish information about its sanctions enforcement activity. Based on our experience, however, there has not been a significant increase in sanctions enforcement activity in recent years.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

The Swiss authorities co-operate with their foreign counterparts provided that co-operation is necessary for the implementation of the imposed sanctions regime, the foreign authorities are bound by official secrecy or a corresponding duty of secrecy, and they guarantee the prevention of industrial espionage within the scope of their activities.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Switzerland does not have restrictions in place that prohibit adherence to other jurisdictions' sanctions or embargoes. However, applicable blocking statutes, secrecy and data protection regulations may restrict compliance with foreign reporting obligations relating to sanctions imposed by other countries or supranational organisations.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

© Law Business Research 2021

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

The Swiss authorities initiate their investigations in general based on their own observations, criminal or other complaints filed by victims or third parties, reports by whistleblowers, media reports and reports from other authorities, including foreign authorities. The criminal authorities and the Swiss Financial Market Supervisory Authority (FINMA) are required to report all offences they become aware of in their official capacity. Investigations are also often triggered by suspicious activity and transaction reports filed with the Money Laundering Reporting Office of Switzerland.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The basis of the data protection regime in Switzerland is the Federal Data Protection Act (FDPA), which is applicable when personal data is processed in Switzerland by a federal authority or a private person (individual or entity). The FDPA is currently under revision to align it with the revised data protection regime of the European Union. The revised FDPA is expected to enter into force in the course of 2022.

Personal data is defined as all information relating to an identified or identifiable person (individual or entity). Under the revised FDPA, data relating to entities will no longer fall within the scope of personal data and the FDPA.

The FDPA requires, inter alia, that personal data only be processed lawfully, in good faith, in a proportionate manner and transparently. Any data processing that does not comply with these processing rules constitutes a breach of the data subject's personal rights. Such breaches are unlawful unless they are justified by the consent of the data subject, by an overriding private or public interest, or by a statutory provision of Swiss law. These core principles will not change under the revised FDPA. However, new or broader duties will be introduced (e.g., documentation, information and notification duties).

In addition, there are a number of additional statutory provisions that regulate or prohibit the process or disclosure of data (e.g., Swiss bank secrecy, professional secrecy and employment law).

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Federal Data Protection and Information Commissioner (FDPIC) is the relevant authority if federal authorities, individuals or entities process personal data in Switzerland. At the moment, the FDPIC has only limited powers; specifically, it has no enforcement powers and cannot impose any fines or sanctions. The FDPIC may issue recommendations that a specific method of data processing be amended or abandoned. If the party concerned does not follow the recommendation or rejects it, the FDPIC may file an action with the Federal Administrative Court. The Court's decision may be challenged before the Federal Supreme Court.

© Law Business Research 2021

If an individual or entity wilfully fails to comply with its information, registration or co-operation obligations under the FDPA, it may be fined up to 10,000 Swiss francs.

Under the revised FDPA, individuals who do not comply with the required duties may be fined up to 250,000 Swiss francs. Corporations may also be fined instead of the responsible individual if a penalty of no more than 50,000 Swiss francs will be imposed and the efforts to identify the responsible individual would be disproportionate compared to the fine.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Internal investigations must be set up in compliance with data protection laws. In practice, the most important data protection issue in connection with internal investigations is the provision that personal data may not be disclosed to recipients outside Switzerland if this seriously endangers the privacy of the data subject. Therefore, personal data may only be transferred to a country with inadequate data protection regulation if it is justified by a statutory provision of Swiss law, the consent of the data subject, or an overriding public interest (an overriding private interest does not suffice). However, Swiss courts only exceptionally acknowledge the existence of an overriding public interest. Under the revised FDPA, the Swiss Federal Council will publish a list of countries with adequate data protection regimes.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Based on data protection and labour laws, employees must be informed about the method, scope, period and purpose of any visual, audio or electronic monitoring. Consequently, any monitoring that is clandestine, or has not been announced in advance, is prohibited and cannot be justified by an overriding interest of the employer.

In addition, there are several criminal provisions that sanction the breach of privacy.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In connection with investigations, dawn raids and search warrants are common tools of the authorities.

In general, houses, dwellings and other rooms not publicly accessible may be searched only with the consent of the proprietor unless a search warrant has been issued. Searches not covered by a search warrant are in general unlawful and evidence obtained in connection with an illegal search is inadmissible unless it is essential to secure a conviction for a serious offence. Other evidence gained from that tainted evidence is in general also not admissible.

© Law Business Research 2021

Search warrants can be challenged before the competent authorities or courts based on both the legitimacy and the scope of the search.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

A request may be made to seal privileged material but this must be done without delay. The authorities must not search the sealed material but they may file a request before the competent courts for the removal of the seal. The court will then review whether the claim of privilege is valid. The court's decision may be challenged before the Federal Supreme Court.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Every individual from the age of 15 and with sufficient mental capacity is compelled to testify before the criminal prosecution authorities and criminal courts unless they have the right to refuse testimony because of a personal relationship (e.g., marriage or kinship), for personal protection (self-incrimination) or to protect closely related persons (e.g., spouses, parents, children or siblings), or owing to official secrecy or professional confidentiality (which applies to, for example, lawyers, members of the clergy and physicians).

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is no specific whistleblowing framework in existence in Switzerland; in particular, there is no specific protection for whistleblowers. A proposal of the Federal Council to improve the protection for whistleblowers was rejected by the National Council in 2019.

Based on Swiss labour law, employees are bound by a duty of loyalty towards their employers. Therefore, they risk legal consequences if they report potential misconduct publicly or to the authorities.

Swiss courts consider a dismissal in connection with whistleblowing to be abusive only if the employee first reported the offence or misconduct internally but if the management did not take appropriate remedial measures. Under Swiss labour law, even an abusive termination is valid and only entitles the dismissed employee to financial compensation of up to six months' salary.

© Law Business Research 2021

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Under Swiss labour law, all employees have a general duty of loyalty towards their employers and an obligation to account for all their activities and work-product during their period of employment. Based on these provisions, it is recognised that employees have to assist with internal investigations conducted by the employer, including providing relevant documents and information, and participating in interviews. In return, employers have the obligation to safeguard the personal rights of their employees. If employees might be subject to criminal prosecution, it is in general advisable to alert them to the right not to incriminate themselves and to allow them to not respond to specific questions. However, there is no uniform opinion or case law regarding this matter. The same applies to the question of whether employees are entitled to have legal representation or a trusted adviser present during interviews.

In general, employees with high-level positions have an increased duty of loyalty towards their employers compared to other employees and thus have increased co-operation obligations in connection with internal investigations.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Under Swiss labour law, an ordinary dismissal is possible at any time without specific grounds, whereas an immediate dismissal requires a material ground. Based on case law, the employer is generally required to investigate the allegations of potential misconduct before dismissing the employee. Otherwise, the dismissal might be considered as abusive and thus entitle the employee to financial compensation.

In practice, corporations tend to suspend employees from work while an investigation regarding their potential misconduct is being carried out.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

An unwarranted refusal to co-operate with an employer's internal investigation constitutes a breach of contractual duties and may entitle the employer to take disciplinary action against the employee who is not co-operating, including, in serious cases, dismissal.

© Law Business Research 2021

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common practice in Switzerland to prepare an investigation plan prior to the launch of an internal investigation. The plan should define in particular the subject matter (i.e., the factual and legal topics to be covered) and the scope of the investigation. Additionally, investigation plans often define investigatory steps, time frames, resources and responsibilities as well as status and final reporting.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no explicit statutory obligation to conduct an internal investigation. However, several provisions in corporate, labour, regulatory and criminal law may require a corporation to investigate potential misconduct so as to avoid liability and sanctions, or to be able to co-operate with the authorities.

Based on their duty of loyalty, employees are in general obliged to report to their superiors if they become aware of potential misconduct within the company. Management is required to inform the board of directors of any misconduct with potential material effects on the corporation.

In recent years, many corporations have introduced whistleblower frameworks that allow employees and third parties to file complaints anonymously.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Under Swiss criminal law, it is illegal to interfere with the course of justice, in particular to tamper with or destroy evidence. In addition, corporations have statutory obligations to preserve documents for certain periods (in general for 10 years). Therefore, corporations are required to have the appropriate systems and directives in place and to provide all employees with clear instructions to prevent material from being destroyed that is subject to an order from a law enforcement authority.

Under the Swiss money laundering regime, receipt of a subpoena triggers due diligence obligations that may result in filing a suspicious activity report with Switzerland's Money Laundering Reporting Office. However, this obligation is only imposed on financial intermediaries.

© Law Business Research 2021

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Unless the company is listed on the Swiss stock exchange exchange and thus is subject to the ad hoc publicity rules (the requirement to disclose information that could have a substantial effect on the market price), there is no obligation to inform the public about an internal investigation or an enquiry from a law enforcement authority.

37 How are internal investigations viewed by local enforcement bodies in your country?

In general, internal investigations are welcomed, or at least tolerated, by Swiss enforcement authorities as long as they do not negatively affect their own investigations. Internal investigations are often a practical necessity for corporations to be in a position to respond to requests from criminal or regulatory authorities.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

In general, internal investigations conducted by Swiss attorneys are subject to the attorney–client privilege. In two recent decisions, however, the Federal Supreme Court called into question the generality of that rule.

In both cases, the clients were financial institutions and the authorities claimed that the invocation of the attorney–client privilege to protect the investigation report and its annexes would constitute a circumvention of statutory documentation obligations under the anti-money laundering legislation. Both decisions have been heavily criticised in the legal community.

Best practice to uphold the attorney–client privilege in connection with internal investigations includes a clear definition of the scope of the investigation and a clear separation between fact finding and legal analysis and advice. If the client is subject to anti-money laundering duties, potential documentation obligations should either be part of a separate investigation stream and report, or explicitly excluded from the scope of the investigation conducted by external counsel.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

With few exceptions, all communications between a client and an attorney and all work-product are subject to the attorney–client privilege, provided that they relate to the attorney's typical professional activities (i.e., advising and representing in legal matters).

© Law Business Research 2021

The protection applies irrespective of the location of the correspondence and documents, that is to say the material does not need to reside with the attorney to be privileged.

In criminal proceedings, privilege cannot be invoked if the attorney is charged in the same context.

Pre-existing documents and materials created outside the scope of an attorney's engagement are not subject to the attorney–client privilege.

Both the client and the attorney are deemed holders of the attorney–client privilege. This means that the client can release the attorney from the confidentiality obligation but the attorney may still refuse to disclose privileged information despite the release.

The attorney–client privilege can be invoked by both individual and corporate clients.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege currently applies only to external counsel. Consequently, communications between employees of a corporation and in-house counsel are not privileged in Switzerland. In connection with the revision of the Civil Procedure Code, it is planned to introduce the attorney–client privilege for in-house counsel under certain conditions.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

According to Swiss procedural laws, the attorney–client privilege applies only to Swiss attorneys and lawyers in EU Member States or countries within the European Free Trade Association who are authorised to practise in Switzerland, unless the client is a target of a criminal investigation. The Swiss Federal Court confirmed this principle in a recent decision.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Swiss authorities cannot require a client or an attorney to waive the attorney–client privilege. If there is a disagreement as to whether specific material is privileged, the competent courts will decide whether the documents may be used by the authorities. If a corporation or individual under investigation seeks leniency but at the same time heavily relies on the attorney–client privilege, this approach might be considered as inconsistent and thus as a lack of co-operation.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

As a general rule, attorney–client communications or work-product may be disclosed to third parties, including Swiss authorities, without waiving privilege. However, the disclosure may lead to factual loss of privilege if the proceedings are public (e.g., court hearings) or the authority is required to share the information with other Swiss or foreign authorities

© Law Business Research 2021

(e.g., mutual administrative or legal assistance). Therefore, it should be decided carefully in each case whether privileged information will be disclosed to Swiss authorities.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

In general, the attorney–client privilege waived on a limited basis in another country can generally be maintained in Switzerland. However, the foreign-based recipient of the privileged information may share the information with the Swiss authorities without informing the privilege holder.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privileges does not exist in Switzerland. Corporations and individuals represented by separate attorneys may share information and work-product with each other without waiving the attorney–client privilege under Swiss law.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

The attorney–client privilege also applies to third parties assisting a Swiss attorney (or an attorney authorised to practise in Switzerland) if the third parties have been engaged by the attorney and the assistance relates to the attorney's typical professional activity (e.g., forensic analysis for advising and representing a client in administrative, civil or criminal proceedings).

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no specific laws on how to conduct an internal investigation. In general, interviewing witnesses is permitted in Switzerland but interviews may be recorded by a camera or audio device only if all participants agree to a recording being made. Violation of this principle constitutes a criminal offence.

According to case law, Swiss lawyers may perform interviews only if there is a factual need for the interview, the interview is in the interest of the client, the lawyer avoids any influence on the interviewee and the interview does not impair investigations by the authorities. These requirements are usually met when a lawyer conducts merely a fact-finding interview in connection with an internal investigation.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Until 2018, the commonly held view was that work-product created by external counsel in connection with internal investigations, including witness interviews or attorney reports,

© Law Business Research 2021

was subject to the attorney–client privilege. This view has been challenged based on two recent decisions of the Federal Supreme Court in 2018 and 2019.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

At the beginning of an interview, the interviewee should be informed about the background of the investigation, the purpose of the interview, any allegations made against the interviewee, and the intended use of the information provided during the interview (in particular whether the information may be shared with authorities). If external lawyers are present at an interview, it should be emphasised that they represent the interests of the corporation and not those of the interviewee.

The questioning should be fair, objective and based on civility and respect towards the interviewee. If it becomes apparent in the course of the interview that an interviewee may expose himself or herself to criminal prosecution, the interviewee should be informed about the right to refuse to testify and the right to seek legal representation. If the authorities are already investigating the matter, it might be advisable to liaise with them to clarify whether they have any objections to the interview.

In general, the aforementioned best practices apply to both employees and third parties. The main difference, however, is that third parties are not under an obligation to assist with an internal investigation or to participate in an interview.

In a recent decision, the Federal Supreme Court concluded that interview notes or minutes are admissible evidence in criminal proceedings even if no *Miranda* warnings were given. However, interview notes or minutes need to meet certain criteria (e.g., bearing the signature of the interviewee and confirming the accuracy of the content or statements) to qualify as documentary evidence and not as mere party allegations.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The structure of an internal interview will depend on the investigation and the person to be interviewed. In general, the interview is typically led by two people. If the interview is conducted by external counsel, a member of the human resources or legal and compliance department is often present. At the beginning of an interview, the interviewee should be informed about the background of the investigation, the purpose of the interview, any allegations made against the interviewee, and the intended use of the information provided during the interview. Documents will be presented to the interviewee if it is necessary or helpful for the line of questioning.

Whether or not an interviewee has a right to legal representation has not been established by the courts to date. In practice, it is the exception that a legal representative for the employee is present at the interview, but it depends on the allegations that are raised.

© Law Business Research 2021

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no general statutory obligation to report potential offences or misconduct to the authorities in Switzerland.

In the financial sector, there are two main reporting obligations. First, supervised entities and individuals must inform the Financial Market Supervisory Authority (FINMA) immediately about any incident, including potential offences or misconduct within their activities, that is of material relevance for the supervision. Second, Swiss financial intermediaries are required to report cases of suspected money laundering to the Money Laundering Reporting Office of Switzerland, based on applicable Swiss anti-money laundering provisions.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Among the many factors to determine whether to self-report are the likelihood that potential misconduct will become public or otherwise known to the competent authorities and the availability of a leniency regime or co-operation bonus. The decision to self-report should be made from a multinational perspective if the potential misconduct relates to more than one jurisdiction.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Before approaching the authorities, a company should have a sufficient understanding of the relevant facts of the misconduct it plans to report. This often requires a preliminary internal investigation. In practice, it is often advisable to contact the authorities informally through external counsel.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Corporations are required to comply with notices and subpoenas unless they challenge them before the competent agencies or courts. There is no obligation to liaise with the law enforcement authorities before responding to notices or subpoenas. In many cases, in practice, however, it is advisable to enter into a dialogue with the law enforcement authorities to get a better understanding of the background, the scope and the next steps of the investigation. A dialogue can also be helpful to clarify potential misunderstandings or ambiguities. Under certain circumstances, the authorities may be willing to amend their

© Law Business Research 2021

notices or subpoenas (e.g., when it would be practically or technically impossible or far too burdensome to provide the authorities with the information or documents requested).

55 Are ongoing authority investigations subject to challenge before the courts?

In criminal law, the initiation of investigations and preliminary proceedings is not subject to challenge before the courts unless the accused person claims that it would constitute a violation of the *ne bis in idem* doctrine (an equivalent of the double jeopardy concept in common law jurisdictions). In practice, the initiation of administrative or regulatory investigations cannot be challenged either.

Once the investigations or preliminary proceedings are under way, procedural orders, compulsory measures and decisions may usually be challenged before the competent agencies or courts.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Swiss and foreign authorities increasingly tend to coordinate a course of action in multi-jurisdictional investigations.

Owing to several Swiss legal provisions, corporations and individuals based in Switzerland are subject to several restrictions when co-operating with foreign authorities, in particular if the requested information and documents include personal data about employees, third parties and clients. Should a foreign authority issue a notice or subpoena, the company must carefully consider whether it may co-operate, may provide only redacted information, needs to obtain an authorisation from the Swiss authorities or should inform the foreign authority that they have to use the channels of mutual administrative or legal assistance.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, the Swiss authorities do not seek production of material that is only available outside Switzerland. In such cases, the Swiss authorities will instead use the available channels of mutual administrative or legal assistance to obtain the material.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Switzerland co-operates with foreign authorities based on mutual administrative or legal assistance and police co-operation through Interpol and Europol.

© Law Business Research 2021

Whether or not assistance is granted depends on whether the applicable requirements are met. In addition, the persons concerned may challenge the decisions of the Swiss authorities to grant assistance before the competent courts.

The sharing of information with Interpol and Europol is in general not subject to challenge before the courts. However, persons may request that information that relates to them is amended or deleted.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Swiss authorities and their staff are bound by official secrecy and may only disclose non-public information they become aware of during the exercise of their official duties, provided the law allows them to do so.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

If a Swiss authority issues a notice or subpoena that would violate foreign law, the company may challenge the order before the competent authority or court. However, Swiss authorities will usually use the available channels of mutual administrative or legal assistance.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Switzerland has several secrecy or blocking statutes that restrict co-operation with foreign authorities. Article 271 of the Criminal Code prohibits and sanctions activities on behalf of a foreign state on Swiss territory unless the competent administrative body has granted an authorisation. In general, Switzerland-based corporations and individuals are thus required to obtain an authorisation from the competent authority if they intend to disclose personal data to foreign authorities based on a notice or subpoena from a foreign authority. Typically, authorisations will not be granted if the channels of mutual administrative or legal assistance are available.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In general, there are no legal risks involved if the production is based on an order or subpoena issued by the Swiss authorities.

In respect of voluntary productions, however, corporations and individuals co-operating with Swiss authorities must be careful not to violate applicable data protection, labour and secrecy laws (in particular, business secrecy and bank secrecy). To reduce their exposure to

© Law Business Research 2021

risk, they can either obtain consent from the data subjects and secrecy owners, or redact the protected information.

Swiss authorities and their staff are bound by official secrecy and may only disclose non-public information they become aware of during the exercise of their official duties, provided the law allows them to do so. Once a case is before a court, however, the proceedings and the oral passing of judgments are, in general, open to the public.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

In criminal proceedings, a corporation may face a fine of up to 5 million Swiss francs. In addition, the court may order the publication of the judgment and the forfeiture or confiscation of assets.

Depending on the offence committed, directors, officers or employees may be punished with a fine (in general, up to 10,000 Swiss francs), a monetary penalty (in general, up to 540,000 Swiss francs) or imprisonment (in general, up to 20 years).

In enforcement proceedings, the Financial Market Supervisory Authority (FINMA) has a wide set of enforcement tools. Inter alia, FINMA may confiscate profits generated or losses avoided through serious violations of financial market laws and regulations by supervised entities or individuals in senior functions, prohibit individuals from exercising a professional activity, withdraw licences and order the liquidation of financial institutions in the event of serious violations. In addition, individuals and entities that do not comply with a FINMA order may be fined up to 100,000 Swiss francs. Finally, individuals who provide FINMA with false information may face a custodial sentence of up to three years or a monetary penalty.

Some supervisory authorities (e.g., the Competition Commission in antitrust and the Federal Office of Communications in telecommunication matters) may impose fines of up to 10 per cent of the average turnover of the corporation in Switzerland during the previous three years.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Debarment from government contracts is currently not a specific sanction under Swiss law. However, if a settlement with a foreign authority may have a relevant effect on the corporation's liquidity, stability, business or reputation, it is advisable to liaise with the competent supervisory authority prior to the settlement.

65 What do the authorities in your country take into account when fixing penalties?

Relevant factors for determining the fines for corporations in connection with any wrongdoing are the seriousness and the number of the offences committed in their commercial activities, the damage caused by the offences, the severity of the organisational

© Law Business Research 2021

inadequacies, the economic ability of the corporation to bear the fine, remedial measures taken (e.g., restructuring measures or reparation payments), the quality of the corporation's co-operation with the authorities during the investigation and previous misconduct.

For individuals, the criminal authorities have to take a variety of aspects into account, including the culpability (i.e., damage caused, conduct and motives), previous conduct and the personal circumstances of the offender as well as potential mitigation factors (e.g., honourable motives, serious distress, dependency and remorse) and the effect that the sentence will have on the offender's life.

Overall, we observe a tendency by criminal authorities to impose higher fines and monetary penalties as well as longer custodial sentences for business crimes.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Neither deferred prosecution agreements (DPAs) nor non-prosecution agreements (NPAs) are available in Switzerland, either for corporations or individuals.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No, since neither DPAs nor NPAs are currently available in Switzerland, either for corporations or individuals.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

According to Swiss case law, journalists are entitled to access settlements with prosecutors unless the access would be contrary to overriding public or private interests. Therefore, corporations should be prepared for media enquiries and coverage once they have reached a settlement. In addition, plaintiffs may use publicly available orders against a corporation to pursue their civil claims because most settlements include an implicit admission of guilt (e.g., payment of reparation or acceptance of the facts).

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Swiss criminal law currently does not provide external corporate compliance monitors as an enforcement tool.

However, the Financial Market Supervisory Authority (FINMA) may engage an independent and suitably qualified person as either an investigating agent or an auditing agent. Investigating agents will be engaged in connection with enforcement proceedings and are responsible for investigating the facts in connection with potential misconduct or

© Law Business Research 2021

implementing supervisory measures ordered by FINMA. Auditing agents will conduct special audits of supervised individuals and entities.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

In connection with criminal investigations and proceedings against corporations or their (former) employees, individuals or entities claiming damages regularly request participation as private plaintiffs. If they are admitted to participate in the criminal proceedings as private plaintiffs, they may have access to the case file, be present during hearings of parties and witnesses, ask questions of the parties and witnesses, submit requests for evidence, and file appeals against orders and the final judgment.

In administrative proceedings, however, in particular in enforcement proceedings conducted by FINMA, private plaintiffs are not parties to the proceedings and thus have no access to the case file and will not be informed about the outcome of the investigation and proceedings.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Swiss authorities and their staff are bound by official secrecy and may only disclose non-public information they become aware of during the exercise of their official duties, provided the law allows them to do so.

Investigations and pretrial proceedings conducted by the criminal authorities are not public. Therefore, the criminal authorities must treat as confidential any information gathered or received during the investigations and pretrial proceedings.

Once a case is before a court, the proceedings and the oral passing of judgments are, in general, open to the public.

FINMA does not usually inform the public about pending investigations. It only publishes information about specific proceedings when this is necessary to protect market participants, to correct wrong or misleading media reports or to maintain the reputation of the Swiss marketplace. If there is a serious violation of the law, FINMA may publish its final ruling and disclose personal data about individuals and entities.

The Competition Commission (COMCO) is required to issue an official press release when opening a formal investigation, stating the purpose of and parties to the investigation. COMCO may publish its decision but the publications must not reveal any business secrets. Corporations named in the decision receive the decision prior to publication and may ask COMCO to redact further information if this is necessary to protect business secrecy or personal privacy.

© Law Business Research 2021

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Communications strategies vary from company to company and will need to be assessed for each situation separately, taking into account various factors, such as the complexity and gravity of the issue or crisis. In complex or severe cases, it has become common to build a communications task force, including external counsel and communications experts, that provides guidance on the communications strategy.

73 How is publicity managed when there are ongoing related proceedings?

The communication strategy depends on the specific circumstances. In general, corporations tend not to comment on ongoing proceedings or only give very high-level comments.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

In general, there is no mandatory obligation to disclose to the market when a settlement has been reached. However, depending on the circumstances (e.g., the penalty amount or the effect on business), the conclusion of a settlement may lead to a disclosure obligation under the ad hoc publicity rules under which publicly listed companies have to disclose any information in their sphere of activity that could have a substantial effect on the market price.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Two new regimes will enter into force on 1 January 2022.

Non-financial reporting obligations

Non-financial reporting obligations on compliance with matters of corporate social responsibility (CSR) (*Transparenz über nichtfinanzielle Belange*), including, but not limited to, environmental and human rights standards will be included as an amendment to the Swiss Code of Obligations (CO) (the Non-Financial Reporting Obligations). Companies of public interest (i.e., public companies as well as banks, insurance companies and other supervised companies in the financial sector) that, with their affiliates in Switzerland and abroad, have (1) at least 500 full-time employees (on average in a year) and (2) either total assets of more than 20 million Swiss francs or revenues of more than 40 million Swiss francs, must report annually on non-financial matters in a stand-alone report. The report must contain information necessary to understand the group's business development, performance and position, and the impact of its activity on environmental (including

© Law Business Research 2021

carbon dioxide emission targets), social, employee, human rights and anti-corruption matters. According to a non-exhaustive list, the report has to include a description of:

- the business model;
- policies pursued (including due diligence applied);
- measures taken and how they are assessed;
- the main risks resulting from the group's own operations and, where relevant and proportionate, from its business relationships, products or services; and
- the main non-financial key performance indicators, in each case with respect to CSR matters.

In accordance with the principle of 'comply or explain', a reporting company may choose not to report in relation to CSR matters with respect to which the group does not pursue policies if the report provides a clear and reasoned explanation therefor. Further, the report may be based on national, European or international reporting standards, such as the Organisation for Economic Co-operation and Development's Guidelines for Multinational Enterprises or the standards of the Global Reporting Initiative or others. Anyone who makes false statements in, or fails to provide, a required non-financial report will be fined up to 100,000 Swiss francs. This means that directors, officers and employees of companies subject to the reporting obligations are the primary subjects of potential criminal liability. However, even if convicted, this does not trigger a registration in the criminal record of the person.

Due diligence obligations

Certain due diligence obligations and transparency obligations (including special reporting obligations on supply chain tracing with regard to minerals and metals) in connection with conflict minerals and child labour will be included as an amendment to the CO (the Due Diligence Obligations) and be further detailed in the Ordinance on Due Diligence Obligations and Transparency in Connection With Conflict Minerals, Conflict Metals and Child Labour (referred to as the Due Diligence Ordinance). The Due Diligence Ordinance is currently available as a preliminary draft only. Under that regime, Swiss companies that (1) import or process a certain amount (the amount imported or processed by group companies to be added) of minerals or metals containing tin, tantalum, tungsten or gold (even as secondary products) from conflict or high-risk areas (excluding recycled metals) or (2) offer products or services where there are reasonable grounds to suspect that child labour was involved, will be subject to certain due diligence obligations with respect to their supply chain (except small and medium-sized enterprises). The obligation under point (2) does not apply if products or services originate from low-risk countries, which will be presumed if the country of origin is one classified as 'Basic' in the Children's Rights in the Workplace Index.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

Currently, the Federal Council is in the process of drafting the Ordinance on Due Diligence Obligations and Transparency in Connection With Conflict Minerals, Conflict

© Law Business Research 2021

Metals and Child Labour (referred to as the Due Diligence Ordinance). A consultation draft has been published and the consultation process was recently completed. As the next step, the Federal Council will review the Due Diligence Ordinance based on the inputs of the consultation process. We do not expect any major changes to the Due Diligence Ordinance before it will be in its final form and enter into effect.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

There has not yet been a notable increase in ESG-related litigation, investigations or enforcement, but we expect some increased activity in line with global trends. The Financial Market Supervisory Authority (FINMA) has made ESG-related topics one of its strategic goals for 2021–2024.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The biggest anticipated change will be brought about by the changes to be made to the Swiss Code of Obligations regarding non-financial reporting and due diligence obligations.

© Law Business Research 2021

24

United Kingdom

Tom Stocker, Neil McInnes, Natalie Sherborn, Andrew Sackey, Laura Gillespie and Olga Tocewicz[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

In July 2020, the Serious Fraud Office (SFO) reached a deferred prosecution agreement (DPA) with G4S Care and Justice Services (UK) Ltd (G4S C&J) in respect of a scheme to defraud the Ministry of Justice in connection with contracts for electronic monitoring of offenders. The quantum agreed in that matter was £38.5 million plus costs but, of perhaps greater significance, was the application of a reduced discount of 40 per cent, said to relate to the delayed nature of G4S C&J's substantial co-operation with the SFO. In September 2020, three former executives of G4S C&J were charged with defrauding the Ministry of Justice. The matter is listed for trial in January 2022.

On 5 February 2021, the UK Supreme Court handed down its judgment in *R (KBR, Inc) v. Director of the Serious Fraud Office* ([2021] UKSC 2), overturning an earlier decision of the High Court, confirming the well-established presumption that UK legislation is generally not intended to have extraterritorial effect. The UK High Court had previously held that the SFO could lawfully require non-UK companies to produce materials

1 Tom Stocker, Neil McInnes, Natalie Sherborn, Andrew Sackey and Laura Gillespie are partners and Olga Tocewicz is a senior associate at Pinsent Masons LLP. The firm's white-collar crime, investigations and compliance team wishes to recognise the valuable contributions made by team members, specifically Stacy Keen and David Hamilton (senior associates), Jonathan Flynn (associate), Alistair Wood and Rebecca Devaney (solicitors), Fiona Cameron (professional support lawyer), employment law specialist Paul Gillen (partner), cybercrime specialist Stuart Davey (partner), data protection expert Anna Flanagan (senior associate), governance and corporate law specialist Tom Proverbs-Garbett (senior associate) and environmental law specialist Fiona Ross (senior associate).

© Law Business Research 2021

held abroad (under its Criminal Justice Act 1987 powers – see further below), provided there was a 'sufficient connection' between the company and the United Kingdom. The Supreme Court ruled that the SFO had not been intended to have such broad extra-territorial compulsory powers, noting that Parliament had instead developed mutual legal assistance to facilitate international investigations and prosecutions. In March 2021, the SFO announced that it had closed its investigation into the activities of KBR, Inc's UK subsidiaries, their officers, employees and agents.

In April 2021, the prosecution by the SFO of fraud charges against two former directors of Serco Geografix Limited (Serco) collapsed. The SFO issued a statement confirming that 'this follows a prosecution review of its disclosure process for the trial, which uncovered errors made in the non-disclosure of certain materials', noting that it was 'considering how best to undertake an assessment to prevent this from happening in the future'. The case again highlights the effects of procedural failings in criminal proceedings, where disclosure obligations remain significant and continue throughout the life of litigation, irrespective of the volume or age of material available or previously disclosed.

In May 2021, the SFO announced it was investigating suspected fraud, fraudulent trading and money laundering in relation to the financing and conduct of the business of companies within the Gupta Family Group Alliance, including its financing arrangements with Greensill Capital UK Ltd. At the time of writing, the investigation remains ongoing.

The SFO also resolved four further investigations by way of DPAs with Airline Services Ltd (agreed on 30 October 2020), Amec Foster Wheeler Energy Limited (agreed on 1 July 2021), and two unnamed companies (agreed on 19 July 2021), embedding the DPA regime as a means, subject to court approval, for corporates and the SFO to resolve cases involving allegations of serious and complex economic corporate crime, avoiding a criminal conviction.

Finally, investigations into the corporate offence of failing to prevent the facilitation of tax evasion continue to gather speed. As at 27 May 2021, Her Majesty's Revenue and Customs (HMRC, the UK tax administration) confirmed it had 14 live investigations into corporates failing to prevent the facilitation of UK tax evasion (an offence introduced as of 30 September 2017). A further 14 live opportunities were also said to be under review, spanning 10 business sectors, including financial services, oils, construction, labour provision and software development.

2 Outline the legal framework for corporate liability in your country.

A corporation can be held criminally liable under the laws applicable to the United Kingdom (the laws of England and Wales, Northern Ireland and Scotland, referred to collectively as UK laws) and there are several ways this can arise, depending on the factual circumstances and the types of underlying conduct.

Typically, corporate criminal offences of strict liability and offences involving a company's vicarious liability for its employees' actions arise for a range of regulatory offences under UK laws. These features of corporate criminal liability are not considered in detail in this chapter as they tend to be less common in relation to financial crime matters, with the exception of offences involving company legislation.

For other types of offences, including fraud and corruption, the law developed the 'identification doctrine' as a means of imputing criminal liability to a corporate. This

© Law Business Research 2021

attributes the knowledge of a corporate's directing mind – the individual or individuals who control the actions of the corporate (for example, its directors or senior managers) – to the corporate itself. In practice this has proved difficult in all but the simplest cases involving small companies with unsophisticated structures. The difficulties are particularly apparent in larger companies or multinationals with more diffuse decision-making among management teams and where complex corporate structures may mean there are numerous reporting lines that would need to be assessed.

In recent years, to meet some of the criticisms of the identification doctrine, the United Kingdom has introduced two types of 'failure to prevent' corporate offences, essentially holding the corporate liable for failing to prevent certain types of wrongdoing, subject in each case to the corporate being able to raise a compliance-related defence (i.e., that it had in place either adequate or reasonable procedures designed to prevent the defined type of wrongdoing occurring). The 'failure to prevent' corporate offence exists under UK laws in relation to bribery (under the Bribery Act 2010) and the facilitation of tax evasion (under the Criminal Finances Act 2017). Both regimes have extraterritorial reach and allow for a company to face prosecution if it fails to prevent bribery or facilitation of tax evasion by a third party performing services either for the company or on its behalf.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The United Kingdom has three legal systems and jurisdictions for criminal law purposes, each of which applies geographically: England and Wales, Northern Ireland and Scotland. The criminal laws of England and Wales and of Northern Ireland are similar, whereas Scots law and procedure is markedly different.

In the United Kingdom as a whole, allegations of corporate offending involve the same criminal process, enforcement agencies and court system as investigations and prosecutions of individuals. As a corporate is a legal rather than a natural person, certain steps vary because of this status (e.g., how it may need to respond to enquiries from a law enforcement authority, how a corporate will appear in court (via counsel) and how it is sentenced if guilty of an offence). Some key law enforcement authorities involved in the regulation, investigation or prosecution of corporates include (not exhaustively) the following:

- SFO – set up with special powers under the Criminal Justice Act 1987 for the investigation and prosecution of large and complex corporate fraud and corruption;
- National Crime Agency (NCA) and local police forces – tends to lead investigations involving significant but smaller-scale or less complex fraud or corporate crime, which is then prosecuted by the Crown Prosecution Service (CPS). The NCA's powers also extend to Northern Ireland;
- The Police Service of Northern Ireland – investigates crimes within the jurisdiction of Northern Ireland. Crimes are then prosecuted by the Public Prosecution Service of Northern Ireland (PPSNI);
- The Police Service of Scotland (Police Scotland) – investigates crimes within the jurisdiction of Scotland. Crimes are then prosecuted by the Crown Office and Procurator Fiscal Service (COPFS);

© Law Business Research 2021

- HMRC – investigates tax-related offending (including money laundering) throughout the United Kingdom, which is then prosecuted by the CPS, the PPSNI or the COPFS, as appropriate. HMRC is also responsible for the enforcement of export controls;
- Financial Conduct Authority (FCA) – regulator of the financial services industry. As a regulator, it can impose civil sanctions for misconduct, but may also prosecute regulated firms or individuals for specific market-related offences, such as insider trading and market manipulation and associated money laundering;
- Competition and Markets Authority (CMA) – investigates anticompetitive behaviour. It may impose civil sanctions but can also prosecute cartel offences;
- Department for Business, Innovation and Skills (the UK government department became part of the Department for Business, Energy and Industrial Strategy in July 2016) and the Department for Economy (Northern Ireland) – these departments respectively investigate and prosecute activities concerning the affairs of companies, including fraudulent trading and breaches of bankruptcy or disqualification orders;
- Information Commissioner's Office – investigates and prosecutes or imposes civil sanctions for data protection offences;
- Health and Safety Executive (HSE) and Health and Safety Executive for Northern Ireland (HSENI) – the HSE investigates and prosecutes or imposes civil sanctions for health and safety offences. In Northern Ireland, it is the PPSNI (not the HSENI) that brings prosecutions. Prosecutions in Scotland are brought by COPFS;
- Office of Gas and Electricity Markets (known as Ofgem) – investigates and prosecutes certain criminal offences under legislation focused on the energy sector;
- Environment Agency, Northern Ireland Environment Agency and Scottish Environmental Protection Agency – investigate and prosecute environmental crime (in Scotland, the prosecution is brought by COPFS and in Northern Ireland by the PPSNI); and
- UK Office of Financial Sanctions Implementation, a department of Her Majesty's Treasury – although not a prosecutor, it has significant additional powers to impose financial penalties for breaches of financial sanctions measures.

Police Scotland has a dedicated economic crime unit, but investigations into serious and complex frauds are overseen by COPFS's economic crime unit. The SFO can also investigate crimes that have occurred in Scotland if they affect other parts of the United Kingdom, but it cannot prosecute cases in or exclusively from Scotland.

There can be concurrent jurisdiction between the SFO and COPFS, particularly with respect to overseas bribery cases and guidance notes, and memoranda of understanding deal with the agreed approaches to co-operation, primacy and guiding principles.

In July 2011, COPFS published its civil settlement guidance, which encourages Scottish and other companies that have committed bribery offences within the jurisdiction of Scotland to self-report to COPFS in return for the opportunity to resolve the case through a civil settlement mechanism. The initiative must be reviewed and approved each year by the Lord Advocate.

In February 2014, following the introduction of DPAs in England and Wales (but not Scotland or Northern Ireland), the SFO and the CPS published a Deferred Prosecution

© Law Business Research 2021

Agreements Code of Practice setting out public interest factors for and against offering a corporate a non-prosecutorial resolution by way of a DPA.

In August 2019, the SFO issued its Corporate Co-operation Guidance as part of its Operational Handbook, which it will use in making charging decisions in relation to allegations of bribery and corruption.

In January 2020, the SFO issued further guidance for corporates and published another chapter of its Operational Handbook entitled 'Evaluating a Compliance Programme'.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Law enforcement authorities must have reasonable grounds to suspect that a criminal offence has been committed to exercise their investigative powers; those suspicions may be founded on evidence or intelligence.

The SFO may investigate any suspected offence that appears, on reasonable grounds, to the director of the SFO to involve serious or complex fraud. The SFO's powers to compel the production of evidence under section 2 of the Criminal Justice Act 1987 can be exercised in any case in which it appears to the director that there is good reason to do so for the purpose of investigating the affairs, or any aspect of the affairs, of any person. The power does not have extraterritorial effect. Additionally, and only in relation to possible bribery and corruption with an international dimension, the SFO may apply a lower test under section 2A of the Criminal Justice Act 1987 to compel the production of evidence if it appears that relevant conduct may have taken place for the purpose of enabling the SFO to decide whether to open a formal investigation.

HMRC has both criminal and civil functions. Its selective criminal investigation policy is a matter of public record.

Criminal investigations into suspected fraud will be considered if civil powers are considered inadequate to address the behaviour or risk, when the severity of the conduct or strong deterrent messaging is required.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Depending on the authority and type of notice, it may be possible to agree informally on a narrower scope of information to be produced without having to formally challenge the lawfulness or scope. Otherwise the recipient may challenge the lawfulness or scope of the notice or production order by way of application to court. Usually this challenge will be by way of judicial review (in Scotland, a bill of suspension), although under certain statutes it may be possible for the company to seek a hearing before the issuing court or tribunal.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

There is the possibility of immunity or leniency for individuals who assist or co-operate in the investigation or prosecution of criminal offences.

© Law Business Research 2021

Section 71 of the Serious Organised Crime and Police Act 2005 (SOCPA) allows certain prosecutors, including the SFO, to grant any person immunity from prosecution in England and Wales or Northern Ireland by issuing a written immunity notice. This notice, which will specify the criminal offences for which no proceedings can be brought, ceases to have effect if the person fails to comply with the conditions contained in the notice. The use of section 71 is relatively rare.

Section 73 of SOCPA provides a means to incentivise assistance from defendants. A defendant who, pursuant to a written agreement with a relevant prosecutor, has provided, or has offered to provide, assistance to an investigator or prosecutor is eligible to receive a reduction in sentence, provided a guilty plea has been tendered. Judges are required to state in open court the sentence that would have been imposed but for the assistance given or offered, unless it would not be in the public interest to disclose that the sentence has been discounted.

Broadly equivalent principles relating to immunity and leniency apply in Scotland under Part 3 of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

The CMA also operates a leniency policy under which businesses and individuals that provide evidence of cartel activity and co-operate with the CMA's investigation can benefit from a reduction in or, in some circumstances, complete immunity from penalties.

7 What are the top priorities for your country's law enforcement authorities?

International corruption and a coordinated global approach to defeat it remains a top priority for the UK government and its law enforcement authorities, together with a desire to harness the expertise of the private sector if the objectives set out in the government's Economic Crime Plan 2019–2022, published in July 2019, are to be achieved.

Commitment to co-operation with other criminal justice agencies, both domestic and international, is echoed in the SFO's Annual Report and Accounts 2020–2021, which identifies one of its primary objectives for the year as to 'develop, and strengthen, constructive relationships with partners both in the UK and internationally'. Strengthening partnerships and exploring opportunities to tackle transnational economic crime in a coordinated and collaborative way remains a priority of the SFO. Equally, intelligence is a key priority, with the SFO's Intelligence Division undertaking a series of threat assessments throughout 2020 to enable it to respond to the changing landscape of economic crime.

During the coronavirus pandemic, there has been an upsurge in those seeking to exploit the situation and take advantage of the many schemes designed to preserve the economy. Law enforcement agencies, including HMRC, have been keen to send a clear message that frauds abusing coronavirus relief schemes will not be tolerated.

A focus on tax evasion led to the introduction of the corporate criminal offence of failing to prevent the facilitation of tax evasion, which came into force in September 2017, and there have been increasing calls to extend the 'failure to prevent' offences to include a schedule of broader economic crimes, such as fraud and money laundering. In November 2020, the government asked the Law Commission to publish a paper providing an assessment of different options for reform. This project is now under way, with the Law Commission reviewing the law relating to the criminal liability of non-natural persons, including companies, and providing options for reform.

© Law Business Research 2021

A further focus is increased transparency of the beneficial ownership of foreign companies investing in UK property or bidding for government contracts. The UK government seeks to make public registers the global norm by the end of 2023 and, on 1 September 2021, restated its commitment to these transparency objectives. Until the public registers are in place, agencies such as HMRC, the SFO and the NCA make use of a comparable 'exchange of notes' requesting protocol.

Effective from 31 January 2018, the Criminal Finances Act 2017 introduced unexplained wealth orders (UWOs) in respect of politically exposed persons or others suspected of involvement in serious crime. UWOs are high court orders following an application from enforcement authorities, such as the FCA, the NCA, the SFO or HMRC, and may be accompanied by an interim freezing order. The respondent is required to set out the nature of interest in the specified property (which must be valued at more than £50,000) and how it was obtained. Failure to respond without a reasonable excuse is met with a presumption that property is recoverable. It is a criminal offence to make reckless or false statements, for which there is a maximum two-year prison sentence and fine. UWOs have been used in four cases, only one of which (based on publicly available information) has resulted in recovery of the assets.

On 27 July 2021, the UK government published its Beating Crime Plan, which includes building capability to deal with fraud, cyber and online crime. It follows the issue by the CPS of its Economic Crime Strategy in March 2021, which set outs its five-year plan focusing on fraud, bribery and corruption, money laundering, terrorist financing, sanctions and market and regulator abuse. Likewise, fraud featured heavily within the FCA's Business Plan 2021–2022, published in July 2021, which explained how the FCA sees its future role and priorities. As part of its Beating Crime Plan, the UK government announced that it will replace Action Fraud, its current national reporting centre for fraud and cybercrime, with an improved national fraud and cybercrime reporting system, and increase intelligence capabilities within the NCA and the national security community to identify the most harmful criminals and organised criminal gangs.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

The 'failure to prevent' offences introduced by the Bribery Act 2010 and the Criminal Finances Act 2017 require corporates to establish, to a civil standard, that they have 'adequate' (bribery) or 'reasonable' (facilitation of tax evasion) prevention procedures in place if they are to avail themselves of the statutory defence. The government has introduced high-level guidance in respect of each enactment to assist corporates and their advisers in assessing what might be considered adequate or reasonable.

Each set of guidance references six principles that should inform an effective compliance programme: top-level commitment; risk assessment; proportional risk-based procedures; due diligence procedures; communications and training; and monitoring and review. In respect of Criminal Finances Act offences, sector-specific guides have also been

© Law Business Research 2021

issued by The Law Society of England and Wales and the financial services sector (and ratified by the government).

The aforementioned six principles provide a useful framework in which to assess the effectiveness of a corporate's compliance programme; however, they are not intended to be prescriptive. A compliance programme should be risk-based and proportionate to the respective risks a company may face.

In January 2020, the SFO published its Guidance on Evaluating a Compliance Programme (the Guidance), which is part of its internal Operational Handbook. The Guidance endorses the six principles outlined above and reiterates that corporates are expected to keep their compliance programmes under review to ensure that they are 'genuinely proactive and effective' and not just a 'paper exercise'.

According to the Guidance, the SFO will consider the effectiveness of a corporate's compliance programme at various stages of an investigation (and, in some cases, after an investigation has concluded). Examples given include whether (1) prosecution is in the public interest, (2) an organisation should be invited to negotiate a DPA, and (3) an organisation has a defence of 'adequate procedures' available against a charge of failure to prevent bribery.

In the context of a DPA, a compliance programme is relevant not only to the assessment of a corporate's suitability for a DPA (a corporate that has implemented a 'genuinely proactive and effective' compliance programme is more likely to be viewed as having reformed and rehabilitated itself), but also the appropriateness of the proposed terms (including monitoring requirements).

The *Airbus SE* DPA approved in January 2020 illustrates the importance of remedial efforts as a condition for any corporate wishing to engage in the DPA process. During the period covered by the DPA, Airbus SE had extensive anti-bribery policies in place and had even secured independent certification in 2012. However, the company accepted that weaknesses in oversight had enabled its compliance measures to be circumvented. Once the wrongdoing was identified, Airbus SE overhauled its compliance programme (seemingly with reference to the six principles referred to above). This resulted in the company putting in place the following remedial steps:

- redesigning its compliance structure and oversight mechanisms;
- rolling out improved and strengthened due diligence processes;
- launching a required company-wide anti-bribery and corruption risk assessment;
- bringing in a newly elected management team; and
- launching internal investigations into the actions of existing and former employees.

When approving the DPA, the court cited these extensive steps, recognising that the overhaul to the management and compliance structure of the business left it 'a changed company to that which existed when the wrongdoing occurred'. This contributed to a 50 per cent reduction in the financial penalty imposed by the DPA.

© Law Business Research 2021

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

Cybersecurity is regulated through a number of statutory regimes. Following the UK's departure from the European Union, on 1 January 2021, Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)) technically ceased to have effect. However, in practical terms, a UK version came into force, which carries much of the EU legislation into UK law, by virtue of the European Union Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. The new legislation upholds the requirement that personal data is 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. Accordingly, organisations that process personal data must have sufficient cybersecurity measures in place to protect against attack. There are mandatory reporting obligations in place where certain attacks happen. The Data Protection Act 2018 (the DP Act) then sits alongside the UK's data protection legislation. The GDPR may also still apply directly to those companies who operate, offer services and goods to individuals, or monitor the behaviour of individuals in the European Union.

Fines have been substantially increased under the GDPR, to up to 4 per cent of annual global turnover or €20 million (whichever is higher) – the UK legislation converts the monetary maximum to £17.5 million, and the Information Commissioner's Office (ICO) has indicated that it intends to use the full force of its powers for the most serious breaches. On 16 October 2020, the ICO issued a monetary penalty notice against British Airways for a data breach affecting more than 400,000 customers, applying the Regulatory Action Policy to determine the appropriate level of fine (£20 million). Just a month later, the ICO issued a monetary penalty notice against Marriott International Inc for £18.4 million after a breach led to the records of around 339 million guests worldwide being affected.

Cybersecurity has far-reaching consequences, however, and a range of other regulators also require notification following a cybersecurity incident; these include the Financial Conduct Authority, the Charity Commission and other professional regulatory bodies.

Cybersecurity is woven into a range of other statutory regimes. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended) regulate providers of public electronic communication services. Service providers are similarly required to take appropriate technical and organisational steps to safeguard the security of their service. The PECR also have mandatory reporting obligations but impose a shorter time frame than the GDPR; within 24 hours of becoming aware of the essential facts. Under the UK's data protection legislation, mandatory personal data breach reports must be made within 72 hours of becoming aware of a breach. Powers open to the ICO in enforcing the PECR include criminal prosecution and a fine of up to £500,000.

Additionally, the Network and Information Systems Regulations 2018 (the NIS Regulations), which came into force on 10 May 2018, govern the threat posed to essential network systems and seek to improve the functioning of the digital economy. The NIS

© Law Business Research 2021

Regulations apply to operators of essential services and relevant digital service providers. They follow a similar principles-based approach to the GDPR, requiring systems operators to ensure appropriate and proportionate technical and organisational measures so as to manage risks to the security of a network.

The United Kingdom has opted to regulate network and information systems according to sector, and there are therefore a range of 'competent authorities' that act as regulators, depending on the specific sector. The NIS Regulations provide for mandatory incident reporting, with a time limit of 72 hours (from becoming aware) for reporting any incident that has a significant effect on the continuity of the essential service. A breach of the Regulations can result in a fine of up to £17 million.

Finally, with the increasing cyber threat from ransomware globally, the National Crime Agency is participating as part of a broad coalition of experts in industry, government, law enforcement and international organisations as part of a Ransomware Task Force, which has launched a comprehensive framework to combat ransomware.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The main regulations relating to cybercrime are the Computer Misuse Act 1990 (the CMA 1990), the DP Act and the Cyber Attacks (Asset Freezing) Regulations 2019 (the 2019 Regulations).

The CMA 1990 has been amended to take account of the developing nature of cybercrime. Offences can be tried summarily or on indictment with a range of maximum sentences, depending on the offence committed.

Although prosecutions have been made over many years pursuant to the CMA 1990, the ICO secured its first conviction in November 2018. The prosecution was followed by an application under the Proceeds of Crime Act and a confiscation order.

The domestic legislation that sits alongside the GDPR is the DP Act, section 170 of which makes it an offence to knowingly or recklessly obtain, disclose, procure or retain personal data without the consent of a data controller and, on indictment, the maximum sentence is an unlimited fine. The offence slightly augments that under the previous legislation (the Data Protection Act 1998). Prosecutions being brought by the ICO currently tend to be pursuant to the 1998 Act in view of the time it takes to investigate and prosecute an offence.

Proceeds of crime legislation can be used as part of the enforcement toolkit; in June 2019, for example, the ICO secured the conviction of a former managing director of a claims management company who had unlawfully obtained and sold personal data. He was sentenced to a fine of £1,050 but the benefit derived from the illegal activity was valued at £1,434,679.60. In view of the defendant's lack of assets, a nominal £1 order was made. That action required the ICO to work in partnership with other agencies; however, on 28 June 2021, the ICO obtained additional powers pursuant to the Proceeds of Crime Act 2002 (References to Financial Investigators) Order 2021, which enable accredited financial investigators to conduct investigations, apply for restraint orders directly and carry out search and seize exercises.

Aside from unauthorised access and use of information, cybercriminals also deploy ransomware to secure a ransom demand. The aim of the 2019 Regulations, which came

© Law Business Research 2021

into force on 11 June 2019, is to address this. Measures under the 2019 Regulations include sanctions, restrictive measures and offences connected with cyberattacks threatening the European Union or its Member States.

The 2019 Regulations apply to UK nationals or any body incorporated in the United Kingdom. They have extraterritorial effect, and their measures are also applicable to conduct wholly or partly outside the United Kingdom that is perpetrated by a UK national, or a body incorporated or constituted under UK law.

The 2019 Regulations restrict interactions with 'designated persons' (adopting a similar approach to sanctions regimes). Dealing with or making funds available to such persons is a criminal offence. The maximum sentence under the 2019 Regulations is an unlimited fine, seven years' imprisonment, or both. At the time of writing, eight natural persons and four legal entities have so far been designated.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The jurisdictional basis of criminal law is generally territorial, as an offence will only be triable in the jurisdiction in which it takes place unless there is a specific provision to the contrary, for instance where specific statutes enable the UK courts to exercise extraterritorial jurisdiction.

Some examples of exceptions are worthy of note. First, under general common law principles, if a substantial part of an offence occurs in the United Kingdom (even if other parts occur outside the territory), the UK courts can have jurisdiction.

Second, under Part I of the Criminal Justice Act 1993, certain fraud, theft, forgery, false accounting, blackmail and cheat offences are triable in England and Wales if a relevant event, or part of the wrongful act within an offence, has occurred in England or Wales. The extension of jurisdiction under this statute also applies to attempts and conspiracies to commit these defined offences.

Third, the Bribery Act 2010 (and prior bribery and corruption legislation) has important provisions to allow law enforcement to investigate and prosecute cases of overseas corruption. A feature of the extraterritorial effect of the Bribery Act 2010 is that it applies to substantive corruption offences in which the acts and omissions are entirely outside the United Kingdom, if these involve UK nationals, others ordinarily resident in the United Kingdom or UK companies, among other defined categories of a party with a close connection to the United Kingdom. The failure to prevent an offence also applies worldwide to corporates that carry on part of their business in the United Kingdom, whether their headquarters are in the United Kingdom or elsewhere.

Sections 45 and 46 of the Criminal Finances Act 2017 followed the 'failure to prevent' model pioneered by the Bribery Act 2010 and created corporate offences of failing to prevent the facilitation of UK or foreign tax evasion. The facilitation of UK evasion will be investigated by Her Majesty's Revenue and Customs, whereas facilitation of foreign tax evasion may be investigated by either the Serious Fraud Office (SFO) or the National Crime Agency (depending on complexity). The offences are extraterritorial in nature,

© Law Business Research 2021

albeit the foreign offence requires a UK corporate nexus and dual criminality in respect of the conduct comprising the tax evasion and the facilitation. It is anticipated that the agencies will work together to develop a uniform understanding of how these offences should be superintended.

In February 2019, the Crime (Overseas Production Orders) Act 2019 received royal assent, allowing UK law enforcement agencies to apply for a court order with extraterritorial effect (an overseas production order), to obtain data stored electronically, directly from communication service providers based outside the United Kingdom.

In October 2020, the Supreme Court heard the appeal in *R (KBR Inc) v. Director of the Serious Fraud Office* and confirmed that a SFO Section 2 Notice does not have extraterritorial effect.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The challenges of dealing with cross-border investigations arise from inconsistencies in the approaches of the various law enforcement agencies and the application of different laws in the relevant jurisdictions.

The principal issues are:

- the differences in the scope and application of legal professional privilege between the jurisdictions, and ensuring that privilege is adequately protected when dealing with document or information requests from the various authorities or when conducting the internal investigation;
- the differences in data protection laws in each jurisdiction, and ensuring that breaches do not occur in the gathering and transferring of data between jurisdictions for the purposes of the internal investigation or responding to requests from a law enforcement authority;
- whether any of the jurisdictions impose a positive statutory obligation to make a formal report once the corporation becomes aware, or begins to suspect, that a crime has been committed (Northern Ireland and Scotland have additional statutes that impose reporting duties that apply in addition to laws that apply UK-wide);
- identifying which authorities may claim that the offending conduct occurred in their jurisdiction as a result of the fact that, with cloud-based communications (email, WhatsApp, iMessage, etc.), offending behaviour, and its impacts, can occur in more than one location;
- whether evidence-sharing or mutual assistance treaties exist between the relevant jurisdictions;
- differing rules surrounding the admissibility of intercepted communications; and
- whether there are sensitivities between the authorities in the various jurisdictions, for example, whether one authority is taking precedence, and if so whether the other authorities accept that position.

Since the expiry of the transition period following the UK's departure from the European Union, the gateways and procedures for sharing intelligence for the purposes of law enforcement co-operation, and entering into joint investigation teams are no longer

© Law Business Research 2021

available to the United Kingdom. Instead, the EU–UK Trade and Cooperation Agreement (TCA), agreed on 24 December 2020, will allow the United Kingdom to use a fast-track process to request extradition of EU nationals (similar to that available to Iceland and Norway), although the process will be more limited than that available under the existing European Arrest Warrant regime. Part 3 of the TCA, containing law enforcement and criminal justice co-operation provisions, includes new arrangements on the sharing of DNA, fingerprint and airline passenger information. However, UK investigators will lose direct, real-time access to sensitive EU databases, such as the Second Schengen Information System, the most widely used automated criminal database in Europe. The United Kingdom has also lost access to the European Criminal Records Information System and will, under the TCA, now have to wait for up to 20 days to obtain the criminal records of EU residents.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The existence of the principle of double jeopardy means that a corporation cannot be prosecuted a second time in the United Kingdom for the same or similar offences on the same facts following a legitimate acquittal or conviction, or other appropriate disposal, such as a deferred prosecution agreement (DPA), by a UK court.

However, the protections for corporates worldwide in relation to double jeopardy principles are more varied and likely to be an area of discussion with law enforcement authorities when a corporate is involved in cross-border investigations in multiple jurisdictions. If the predicate offending has been disposed of in one jurisdiction, double jeopardy will not preclude UK authorities from prosecuting ancillary or incidental offences, such as record-keeping or money laundering offences that occurred in the United Kingdom. Nevertheless, there is scope to engage with international law enforcement agencies with close ties to UK enforcement agencies or mutual legal assistance arrangements with the United Kingdom (or both) to ensure that, in practice, one agency takes primary responsibility for the investigation and enforcement, to avoid any undue prejudice when a case spans multiple jurisdictions. Notwithstanding this, frequently corporates will be expected to respond to enquiries simultaneously from agencies inside and outside the United Kingdom, and there are no general, formal rights on the part of a company to seek to stay a UK investigation pending the outcome of a foreign investigation or set of criminal proceedings that may have commenced prior to the UK law enforcement agencies becoming involved.

There is no UK policy analogous to the 'anti-piling on' policy that exists in the United States. However, in situations of concurrent jurisdiction, there are memoranda of understanding between the various law enforcement and regulatory authorities in the United Kingdom. These provide a framework for co-operation between organisations that have

© Law Business Research 2021

(or may have) jurisdiction to prosecute an offence and for determining 'primacy' to investigate and prosecute offences.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are becoming increasingly common. In November 2015, a DPA was agreed between the SFO and Standard Bank PLC, which was coordinated with the settlement between Standard Bank and the US Securities and Exchange Commission.

In January 2020, the SFO entered into a record-breaking DPA with the global aerospace company Airbus SE. This is the world's largest global resolution for bribery to date.

In June 2021, Scotland-based engineering company John Wood Group reached a US$177 million global bribery settlement with authorities in the United States, the United Kingdom and Brazil, concluding legacy bribery and corruption investigations into Amec Foster Wheeler companies.

The SFO will also reference the assistance it receives from foreign authorities at the conclusion of any successful prosecution.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Law enforcement authorities generally seek to co-operate with counterparties in foreign jurisdictions. Usually at the outset of an investigation, the authorities will agree whether one jurisdiction should take precedence in the investigation and prosecution of the matter (e.g., if the majority of the alleged misconduct took place in that jurisdiction or in the jurisdiction of incorporation) or agree which aspect of a larger cross-border enquiry involving a corporate each will lead on if the case involves a number of components.

Even if it is agreed that the predicate offending in a matter should be prosecuted in one particular country, incidental offences, such as books and records offences, can still be prosecuted in the other jurisdictions.

Ultimately, UK authorities are responsible for the conduct of their own investigations and prosecutions. The extent to which a decision by a foreign authority would influence a UK investigation will depend on the particular facts of the matter, the relationship between the UK and foreign authorities, and the relationship between the United Kingdom and the other country on a state or institutional level.

DPAs agreed in the United Kingdom often also include terms that require the recipient to provide co-operation with the SFO on all investigations and pre-investigations and prosecutions for the term of the DPA, including co-operation with foreign law enforcement and regulatory authorities or agencies on all matters relating to the conduct in question.

© Law Business Research 2021

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

On 31 December 2020, the United Kingdom introduced autonomous sanctions regimes following its departure from the European Union. These UK regimes are introduced under the Sanctions and Anti-Money Laundering Act 2018.

Prior to 31 December 2020, with the exception of domestic sanctions focused on counterterrorism, sanctions in the United Kingdom stemmed from the European Union (including those implementing the sanctions imposed by the United Nations).

The UK and EU sanctions regimes broadly align although they are not identical. For example, the UK concepts of brokering and finance-related services extend explicitly to activities beyond the EU counterparts. The United Kingdom also maintains a sanctions regime, under the Global Anti-Corruption Sanctions Regulations 2021, to prevent and combat serious corruption, while at present there is no EU equivalent.

The main types of sanctions the United Kingdom imposes are:

- trade sanctions, including restrictions relating to certain items (most commonly military and dual-use items and those that can be used for internal repression or to monitor and intercept communications), certain sectors and the provision of certain services (these sanctions are in addition to the UK's general export control laws);
- financial sanctions, including asset freezes; and
- immigration sanctions, known as travel bans.

There may be specific exceptions under which it is possible to engage in an activity that would otherwise be prohibited. It may also be possible to get a licence or authorisation permitting activities that would otherwise be prohibited, although they are generally available in limited circumstances.

A principle of sanctions regimes is the prohibition on knowingly and intentionally participating in activities that have the object or effect of circumventing any sanctions laws or enabling or facilitating the contravention of those laws.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The Department for International Trade implements trade sanctions and other trade restrictions. Her Majesty's Revenue and Customs has primary responsibility for the enforcement of export controls. The UK Office of Financial Sanctions Implementation (OFSI), which is part of HM Treasury, implements and enforces financial sanctions. The Home Office implements and enforces immigration sanctions.

The potential consequences for breaching sanctions laws are severe, including unlimited criminal fines, periods of imprisonment for individuals, the disgorgement of any profits and reputational damage.

The 2017 Policing and Crime Act introduced civil penalties for breaches of financial sanctions, available in cases where it is not in the public interest to prosecute.

© Law Business Research 2021

To date, OFSI has imposed five civil penalties, against Raphaels Bank (February 2019), Travelex (UK) Ltd (May 2019), Telia (October 2019), Standard Chartered (April 2020) and TransferGo Limited (August 2019). The imposition of the penalty against TransferGo Limited demonstrated that a failure to appreciate the application of financial sanctions is no defence.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Prior to its departure from the European Union, the United Kingdom had a leading role in developing the EU sanctions policy. There are instances in which the United Kingdom has coordinated the sanctions that it imposes with, most commonly, the European Union, Canada and the United States.

OFSI has an international engagement branch that is leading an 'initiative to help promote robust financial sanctions implementation on the world stage, not only through bilateral and multilateral meetings/events but also through technical assistance to other governments'.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Council Regulation (EC) No. 2271/96 protecting against the effects of the extraterritorial application of legislation adopted by a third country and actions based thereon or resulting therefrom (the EU Blocking Regulation) forms part of the retained EU law applying in the United Kingdom.

The EU Blocking Regulation currently applies to certain sanctions imposed by the United States in respect of Cuba and Iran (referred to as the listed extraterritorial sanctions). The Regulation was updated in August 2018 following the United States' withdrawal from the Joint Comprehensive Plan of Action known as the 'Iran deal'.

The EU Blocking Regulation has the following four main components:

- UK persons (UK nationals and UK-incorporated entities) and those in the territory of the United Kingdom are prohibited, without authorisation from the Secretary of State for International Trade, from complying, either directly or through a subsidiary or other third party, actively or by deliberate omission, directly or indirectly, with any requirement or prohibition with the listed extraterritorial sanctions.
- UK persons whose economic or financial interests are directly affected by the listed extraterritorial sanctions must inform the Secretary of State for International Trade of this within 30 days. In the case of UK businesses, the reporting obligation rests with directors, managers and others with managerial responsibility.
- Judgments or decisions of non-UK courts, tribunals or administrative authorities giving effect to the listed extraterritorial sanctions are not enforceable in the United Kingdom. This is intended to shield UK persons from, for example, the effects of any decision requiring seizure or enforcement of any penalty in the United Kingdom based on the listed extraterritorial sanctions.

© Law Business Research 2021

- UK persons 'engaging in international trade and/or the movement of capital and related commercial activities between the UK and third countries' are entitled to recover damages for harm caused to them by the application of the listed extra-territorial sanctions. Recovery can take the form of seizure and sale of the assets of the persons causing the damage, their representatives or intermediaries.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

It is a criminal offence to breach the prohibition or fail to comply with the reporting obligation provided in the EU Blocking Regulation. This offence is punishable by an unlimited fine.

If a UK national or incorporated entity wishes to comply with any listed extra-territorial sanctions in the Blocking Regulation, authorisation must first be obtained from the Secretary of State for International Trade. In considering applications, the Secretary of State will consider the 14 criteria set out in Commission Implementing Regulation (EU) 2018/1101. Authorisation is effective on the date when it is notified to the applicant.

To date, no UK nationals or UK-incorporated entities have been prosecuted for a breach of the EU Blocking Regulation.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

In addition to the normal means for identifying misconduct, such as audits, assurance procedures and whistleblowing, UK companies can become aware of allegations of misconduct through insolvencies, cybercrime or data breaches (e.g., the *Unaoil* and *Panama Papers* cases) and due diligence carried out in relation to commercial transactions, including mergers and acquisitions.

Allegations may also arise in hearings, such as employment tribunals and litigation proceedings.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The United Kingdom implemented the Data Protection Act 2018 (the DP Act) to complement the EU General Data Protection Regulation (GDPR). The GDPR has direct effect across all EU Member States and applies directly to all organisations processing personal data within the Union. However, it allows each Member State limited opportunities to make provisions for how it applies in that country. The DP Act essentially provides the details of local derogations, such as law enforcement processing. The two must therefore be read side by side. This new legislation supplements existing UK laws such as the Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000, and directly applicable EU legislation, such as the Privacy and Electronic Communications Regulations.

© Law Business Research 2021

Since the departure of the United Kingdom from the European Union, primarily, data protection is governed by the European Union Act 2018, The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and the DP Act. The UK data protection legislation succeeds the GDPR and must be read alongside the DP Act. This legislation supplements existing UK laws such as the Freedom of Information Act 2000, the Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016 as well as legislation such as the Privacy and Electronic Communications Regulations. However, on 10 September 2021, the UK government launched a consultation on proposed reforms to the UK data protection regime ('Data: a new regime').

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The power for enforcement of the data protection regime rests with the Information Commissioner's Office (ICO). The ICO has a range of enforcement powers, the most notable being the imposition of large fines. However, in addition to this power to issue fines, the ICO has a range of other powers, including information notices, assessment notices, enforcement notices, and statutory powers of entry and inspection. In June 2021, the ICO gained new powers pursuant to the Proceeds of Crime Act 2002 (References to Financial Investigators) Order 2021 to enable it to apply for restraint orders as well as to carry out search and seizure exercises where it believes cash has been obtained through, or intended for use in, criminal activities.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Typically, a considerable amount of evidence will be reviewed in the course of any internal investigation and must be handled carefully to ensure compliance with the DP Act. It is very likely that it will be necessary to conduct a data privacy impact assessment before processing any information. Decisions taken with regard to the processing and disclosure of data should be made in accordance with the DP Act, and all reasons for those decisions should be documented. If any of the data reviewed contain or may contain personal data, particularly sensitive personal data (now 'special categories'), extra care should be taken. Firms should seek legal advice with regard to what additional measures should be taken in relation to this material. This includes whether redaction of any personal information is required and whether this would be an appropriate mechanism to avoid any data protection breaches.

Further, extra care should be taken in circumstances where there may be a transfer of the data outside the United Kingdom and European Union. Data flows between Europe and the United Kingdom are permissible as the EU Commission published, on 28 June 2021, two adequacy decisions in respect of the United Kingdom. However, transfer of personal data to the United States needs particular review following the European Court of Justice decision in the *Schrems II* case (July 2020), which invalidated the EU–US Privacy Shield. International transfers generally have also been affected by *Schrems II*, as the case had some further implications for the use of the EU Standard Contractual Clauses (SCCs). The ICO has published a draft UK addendum alongside a new draft

© Law Business Research 2021

international data transfer agreement, which is effectively the UK equivalent of the EU SCCs. The European Data Protection Board has recommended that firms conduct a risk assessment as to whether SCCs provide enough protection within the local framework, whether the transfer is to the United States or elsewhere.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

A range of factors must be taken into account when considering the monitoring of employee communications. These typically fall into two categories:

- reviewing emails sent and received by an employee; and
- intercepting emails before receipt.

In relation to the review of emails sent and received by an employee, the situation broadly involves considerations under the GDPR, the DP Act and the Human Rights Act 2000. The processing of emails through review will require an employer to consider the extent to which it can satisfy a lawful condition of processing under the GDPR with balancing the data subject and privacy rights. However, consent is not typically a basis on which the processing would take place as, under the GDPR, consent has to be given freely and the ICO has stated that it is unlikely that consent could be so considered in an employer–employee relationship in view of the imbalance of power.

If monitoring does take place, this will often be overt monitoring, in that the employer will set out in its information technology use and privacy policies that it retains the right to access emails and messages sent and received on devices used by employers.

The ICO issued guidance prior to the implementation of the GDPR. As yet this has not been updated but recommends that covert monitoring takes place only in exceptional circumstances; for example, for the detection of crime.

It is essential, if monitoring is taking place, that the employer ensures that it is proportionate and undertaken only for as long as is necessary.

The GDPR sets out circumstances in which it is mandatory to conduct a data protection impact assessment, which includes assessing when processing is likely to result in a high risk to data subjects. As a matter of good practice, it may be prudent to work through a risk assessment prior to processing even when the high threshold has not been triggered, so that essential security and data minimisation measures are considered and adopted where necessary.

Up to 27 June 2018, the Provisions of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) governed the interception of electronic communications during transmission. These have been replaced by the Investigatory Powers Act 2016 (IPA) and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356) (the 2018 Regulations).

Under the IPA, it is a criminal offence to intercept communications without lawful authority. Although the 2018 Regulations include the detection of crime as authorised conduct in certain circumstances, given the criminal implications of interception without

© Law Business Research 2021

proper authority, every case must be assessed on its merits to ensure that the relevant standards are met.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Authorities that investigate corporate crime, such as the Serious Fraud Office (SFO) or Her Majesty's Revenue and Customs (HMRC), often conduct dawn raids of business or residential premises under the authority of a search warrant issued by a court. A raid is often undertaken in conjunction with a local police force.

When a raid is carried out under a warrant (searches without warrant are permissible subject to overarching statutory controls), the authority may only search the premises specified in the warrant.

In England, Wales and Northern Ireland, certain categories of material, such as confidential journalistic material or personal records created in the course of a business (e.g., patient records in a medical practice) cannot be seized during a raid without additional authorisations being obtained, in some circumstances from particular courts. Different rules apply in Scotland.

In the United Kingdom as a whole, legally privileged material cannot be seized unless it was created with the intention of the furtherance of a crime (the crime-fraud exception) or is inextricably linked to other, seizable material. If that is the case, material can be seized but must be sifted to exclude as far as possible any privileged material from the investigating team at the law enforcement agency. In England and Wales, a typical approach is for material subject to a claim of legal privilege to be examined by an independent lawyer before it is examined by the investigating team (and any privilege material excluded). The use of this power is also subject to the Criminal Justice and Police Act 2001, which entitles a corporate's legal representative to be present at a review of the material and apply to a judge for the material to be returned. In Scotland, there is no statutory framework for dealing with privilege issues and it may be necessary to apply to the courts for the seizure of privilege material to be suspended.

The Competition and Markets Authority (CMA) may conduct a dawn raid of business premises without a warrant.

Some authorities have additional powers that can be exercised during a dawn raid; for example, the SFO and the CMA may compel a person to answer questions relevant to the search, such as regarding the location of certain documents. These powers, and equivalent sanctions, are mirrored by means of disclosure notices issued pursuant to sections 60 to 70 of the Serious Organised Crime and Police Act 2005, although the prosecutor rather than the investigator must sanction the use of these notices.

If there are significant errors in either the process of obtaining a warrant or authorising a raid, or in the execution of a raid, the warrant can be challenged by judicial review and rendered unlawful and the material seized during the raid could be rendered inadmissible or returned to the subject.

© Law Business Research 2021

The Law Commission is reviewing the law governing search warrants. A consultation on the issue closed on 5 September 2018. In a report laid before Parliament in October 2020, the Commission made 64 recommendations to strengthen law enforcement powers, improve the search warrant process, clarify the rules around electronic material and strengthen safeguards for those being investigated.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

As a general rule, legally privileged material cannot be seized during a dawn raid unless the crime-fraud exception applies or where it is inextricably linked to seizable material, in which case other safeguards should be adhered to. These include the sifting of material, by an independent legal team, to exclude as far as possible any privileged material from the investigating team at the law enforcement agency. However, should certain competition investigations also involve the European Commission, note that it does not regard advice from in-house lawyers as legally privileged. Following the United Kingdom's departure from the European Union, the Commission can no longer conduct dawn raids in the United Kingdom nor request that the CMA does so on its behalf (other than in relation to cases brought prior to the end of the transition period). If there is any co-operation between the CMA and European Commission, the CMA would conduct the raid and UK rules on privilege would apply. The European Commission can still send information requests to UK companies under Article 18 of Council Regulation (EC) No. 1/2003 on the implementation of the rules on competition and, where those requests ask for documents containing legal advice, the Commission's approach to privilege would apply.

In England, Wales and Northern Ireland, the authorities that investigate corporate crime are routinely accompanied during raids by an independent lawyer specifically tasked with reviewing on-site any material that a company asserts as privileged. It is important, therefore, to be aware of where privileged material is likely to exist so that assertions can be made before items are seized.

If there is a dispute regarding privilege that cannot be resolved in situ, the authority will seize the material by sealing it in an opaque bag for review by an independent lawyer or the court at a later date. The company is entitled to have its legal representative present during that review.

Digital devices containing both privileged and non-privileged items that cannot be separated may be seized or imaged during a raid. In practice, the privileged material will then be quarantined by digital forensic experts within the authority by applying search criteria provided by the company.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

In England, Wales and Northern Ireland, there is a qualified right of silence when being interviewed as a suspect, and a defendant in a criminal trial has a right not to give evidence.

© Law Business Research 2021

In both situations, the right is qualified as, in certain circumstances, adverse inferences can be drawn from this silence.

However, in Scotland the right to silence is not qualified and no negative inference can be drawn from an interviewee's refusal to answer questions.

A right of silence does not apply when an authority such as the SFO, Financial Conduct Authority or CMA (or HMRC or the police when powers under the Serious Organised Crime and Police Act 2005 are in play) exercises specific statutory powers by issuing a notice compelling a witness to answer questions or produce documents. Failure to comply with such a notice without a reasonable excuse can constitute a criminal offence. However, the contents of a compulsory interview under these powers cannot be used against the individual except in a prosecution specifically for making a false or misleading statement in that interview.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Public Interest Disclosure Act 1998 and the Public Interest Disclosure (Northern Ireland) Order 1998, as amended, combined with the Employment Rights Act 1996 and the Employment Rights (Northern Ireland) Order 1996, offer statutory protections to whistleblowers.

It should be noted that the protection afforded for whistleblowers is wider than the typical definition of 'employee' or 'worker'. There are a number of individuals who are now included for protection who would not normally be, including: homeworkers; self-employed doctors, dentists, ophthalmologists and pharmacists in the National Health Service (NHS); agency workers; police officers; student nurses and student midwives; job applicants in the NHS. It has also been held that an equity partner in a limited liability partnership law firm was a worker for whistleblowing purposes (*Clyde & Co LLO v. Bates van Winkelhof* [2014] UKSC 32). It was also held in *Gilham v. Ministry of Justice* [2019] UKSC 44 that judges, as office holders, should be afforded the protection, which could have implications regarding protection for other office holders.

The dismissal of an employee will be automatically unfair if the principal reason for dismissal is that the individual has made a qualifying 'protected disclosure'. Workers (as defined above) and employees are also protected from detrimental treatment (e.g., harassment, reduction in pay or dismissal) on the ground that they have made a qualifying protected disclosure.

There is no requirement for a minimum period of service nor is there any financial cap on the amount of compensation that can be awarded. An employee alleging automatic unfair dismissal on the grounds of being a whistleblower may make an immediate application for interim relief, which may result in effective reinstatement. A successful automatic unfair dismissal claim could also result in the individual being reinstated as an employee, although this is rare.

There are no financial incentive schemes in the United Kingdom for whistleblowers.

© Law Business Research 2021

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Suspension pending investigation

Employment legislation does not specifically deal with suspension but case law and guidance issued by the Advisory, Conciliation and Arbitration Service (ACAS, a public body funded by the UK government), in the form of the ACAS Code of Practice on Disciplinary and Grievance Procedures (the ACAS Code), requires that employees be suspended only when this is necessary and that the period of suspension be as short as possible and kept under review. Employees should be informed, preferably in writing, of the nature of the allegations made against them (whether in relation to an internal or external investigation) and, in most cases, suspension should be on full pay and with no loss of benefits. Any failure to follow these principles can result in a breach of the ACAS Code and could be a repudiatory breach of contract. In Northern Ireland, similar provisions apply, pursuant to the Labour Relations Agency, Code of Practice on Disciplinary and Grievance Procedures (the LRA Code). An employee should not be suspended for having raised a protected disclosure as this could be deemed a detriment. When it is necessary to suspend any employee alleged of misconduct, the employer should check whether it has an express right (or, depending on the industry, an implied right) to suspend the employee as, without this, there could be a breach of contract.

The right to a fair hearing

The disciplinary process should be carried out in accordance with the ACAS Code. As a minimum, it should include an investigation to establish the facts before proceeding to a disciplinary hearing (assuming there is a case to answer). In good time ahead of a disciplinary hearing, the employee must be informed of the allegations against him or her and the right to be accompanied at the hearing by a colleague or a trade union representative. During the hearing, the accused should be given a full opportunity to answer the allegations before any decision is made by the employer.

Employers should carry out their own disciplinary process irrespective of any third-party finding of guilt (e.g., by the police). The employer is still required to follow a fair disciplinary process (in accordance with the ACAS Code) as far as possible. As stated above, in Northern Ireland, compliance with the LRA Code (rather than the ACAS Code) is required but also note that, unlike in Great Britain, statutory dismissal procedures have been retained.

These requirements can be relaxed when employees do not have the requisite length of service with their employer to bring an unfair dismissal claim (two years in Great Britain and one year in Northern Ireland); however, it is best practice to follow a fair process in dismissals, to avoid allegations of whistleblowing or discriminatory treatment.

The right not to be unfairly dismissed

All employees with the requisite length of service have the right not to be unfairly dismissed. In the case of a successful claim, an employment tribunal can order reinstatement or re-engagement, or award compensation. In most cases in Great Britain,

© Law Business Research 2021

compensation is capped at one year's pay or £89,493 (whichever is lower) plus a basic award of up to £16,320. In Northern Ireland, the one-year pay cap does not apply and unfair dismissal compensation is capped at £89,669, plus a basic award of up to £16,980, although in certain situations, employees can argue that this compensation cap should be disapplied.

The requirement for length of service and the statutory caps on compensation do not apply when the employee successfully alleges that the principal reason for dismissal is that the individual made a qualifying protected disclosure.

Company director considerations

Directors may also be employees (in which case the above will apply in tandem with any specific issues regarding directors' duties). A director who is not an employee (i.e., a non-executive director) will not be subject to the above rules. However, directors are subject to general duties, which are set out in the Companies Act 2006, contained within a company's articles and may also be set out in any letter of appointment. The company's articles and any relevant letter of appointment will include provisions regarding the removal of a director who has acted in breach of one or more of his or her duties under the Companies Act. There are additional regulations that apply to directors of public companies.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Rights regarding suspension, the right to a fair hearing and the right not to be unfairly dismissed all apply to employees who may have engaged in misconduct. There is no strict employment law requirement to suspend or discipline those suspected of misconduct; that is a decision for the employer. Some heavily regulated employers, such as those within the financial services sector, may have increased obligations around suspension and disciplinary action where employees carry out regulated activities. In some cases, an employee's misconduct must be reported to the regulator. Employees may also be regulated themselves and will have specific obligations towards the regulator.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

In general, a request to participate in an internal investigation will be a reasonable management instruction and any unreasonable refusal to engage in this process may constitute misconduct in itself. Whether or not an employer could fairly dismiss in these circumstances will depend on the whole context and in particular, the seniority of the employee. At all times, it is important that the employer does not interrogate or put pressure on the employee to make admissions of guilt, and a range of safeguards as to how the investigation is conducted should be considered, to ensure fairness to the employee.

© Law Business Research 2021

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is good practice to prepare an initial scope of an internal investigation, potentially with a written investigation plan, with target deadlines and a clear set of tasks where possible, before commencing the investigation proper, setting out:

- its purpose;
- the issues to be investigated;
- the client, and who within an organisation can provide instructions on behalf of the company;
- the investigation team and reporting lines;
- how legal privilege will be established and maintained (e.g., the investigation team is instructed by and reports to a lawyer);
- how digital and hard copy material will be collected and preserved;
- how staff interviews will be conducted; and
- any other necessary immediate controls or steps, such as ceasing all future payments to third parties under suspicion.

The scope of an internal investigation and the client team may need to be kept under review, depending on factual findings and other developments that are possible at different stages in the investigation.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are generally no formal legal obligations on a company to conduct an internal investigation into its own affairs. However, conduct rules applicable to some companies by the bodies that regulate them may mean an internal investigation is strongly recommended or even required.

The company should also consider whether a money laundering report is needed in accordance with the Proceeds of Crime Act 2002 (UK-wide application) and whether any additional report is required for the police in Northern Ireland or Scotland to comply with specific legislation that is applicable in those jurisdictions. In addition, the company should:

- stop the offending behaviour, otherwise the company could be exposed to a risk of criminal liability itself for allowing potential offending to carry on unchecked and without investigation;
- if there are grounds for suspecting (where that suspicion is more than merely fanciful) that funds relating to a future transaction may be tainted as the proceeds of crime, consider making a Defence Against Money Laundering report to the National Crime Agency, requesting a defence to proceed with that transaction;

© Law Business Research 2021

- preserve all documents and material relevant to the issue. Failure to preserve evidence could also impede a later criminal investigation, leaving the company at risk of criticism from, or undermining its ability to demonstrate its co-operation with, the authority. Note also that it can be a criminal offence to undertake any acts that can affect the administration of justice. Relevant conduct may include destroying, falsifying, concealing or disposing of relevant documents when a person knows or suspects an investigation of serious or complex fraud is already being, or is likely to be, undertaken by certain law enforcement agencies; and
- take remedial or preventive action to ensure that the offending behaviour cannot occur in the company again.

If a company has failed to take any steps to address an allegation of bribery or facilitation of tax evasion, it is unlikely that it would be able to rely on the 'adequate or reasonable procedures' defence in the event of a prosecution of corporate failure to prevent under the Bribery Act 2010 or Criminal Finances Act 2017.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

On receipt, the notice or court order should be sent immediately to the appropriate person within the business whose function is to deal with this type of external matter (usually within the legal department). All steps should be taken to ensure that evidence that may be relevant for production under the notice or court order is not deliberately or inadvertently lost, destroyed or altered, and that any individuals who may be involved in possible wrongdoing are not tipped off. The exact scope of the request should be determined and clarifications sought if the scope is unclear. The deadline for responding should also be diarised. It is advisable to seek external legal advice if the legal department is inexperienced in dealing with such matters.

Once reviewed for relevance, the results should be checked for privilege, and copies retained of anything provided to the authorities.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement.

Under the UK Listing Rules, publicly listed companies must issue a market announcement of any major new development that may affect their business without delay, if the development may lead to a substantial share price movement. A notice compelling the provision of documents would be unlikely to require an announcement, but confirmation from the authority that the company was a suspect in a criminal investigation would be likely to require an announcement.

Organisations that are authorised by the Financial Conduct Authority also have an obligation to disclose to it anything relating to the firm of which it would reasonably

© Law Business Research 2021

expect notice. This would include breaches of UK laws and regulations, civil, criminal or disciplinary proceedings against a firm and fraud, errors and other irregularities.

Public companies are also required to complete a fraud and error declaration as part of their audit process, expressly referencing not only material misstatements but suspicions of fraud or control failures. A person commits a criminal offence pursuant to section 501 of the Companies Act 2006 if he or she knowingly or recklessly make a misleading, false or deceptive statement to an auditor.

37 How are internal investigations viewed by local enforcement bodies in your country?

UK authorities have publicly stated that they are not opposed to internal investigations that are carried out in a manner that would not impede a criminal prosecution. They expect data-gathering exercises to be carried out promptly and covertly and to be coordinated across multiple sites simultaneously. 'Covert' in this context is intended to ensure potential suspects in a later criminal investigation are not tipped off prior to data collection and so given an opportunity to destroy or delete incriminating material. It does not mean that companies should conduct internal investigations in a manner that involves unlawful surveillance or data-gathering techniques (whereby they could be separately liable for other offences). Data collections should be forensically sound, preserving metadata. All procedures used to gather and image data should be recorded and then fully disclosed to the relevant law enforcement authority.

Additionally, UK authorities expect that full and accurate accounts are made of any witness interviews and, in some circumstances, consideration may need to be given to whether certain interviews should be conducted at all. This is particularly important if there is a risk of criticism that a corporate conducted an interview knowing that a law enforcement agency would wish to speak to a witness first and obtain a first account from a witness prior to any internal investigation or review.

The Serious Fraud Office has repeatedly said that it expects to be given interview notes by corporates seeking to demonstrate co-operation in their investigation. While this is tempered to an extent by an acknowledgement that disclosure is not required when legal professional privilege applies, when such a claim is without foundation, co-operation is likely to be cast into doubt in the absence of such a disclosure.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal professional privilege has traditionally been claimed over various aspects of internal investigations, which has increasingly been disputed by law enforcement authorities. However, in a 2018 Court of Appeal case, Eurasian Natural Resources Corporation Limited (ENRC) successfully repelled a challenge by the Serious Fraud Office (SFO) relating to claims of privilege by the corporation. The SFO sought to challenge claims

© Law Business Research 2021

to privilege by ENRC regarding various documents that were produced by lawyers and forensic accountants during an internal investigation into allegations of bribery and corruption that had arisen from a whistleblower report. The documents in question fell into four categories:

- category 1: notes taken by lawyers of interviews conducted during an internal investigation;
- category 2: materials generated by forensic accountants as part of a 'books and records' review;
- category 3: documents, such as presentation slides, containing or surmising factual evidence, that were used by lawyers to present to ENRC; and
- category 4: emails between a senior executive and the head of mergers and acquisitions at ENRC, who was a Switzerland-qualified lawyer.

The Court of Appeal held that documents falling into categories 1, 2 and 4 were protected by litigation privilege. The High Court had already held that the factual updates provided in category 3 were protected by legal advice privilege.

In short, the Court of Appeal held that a criminal investigation by the SFO could be 'litigation' for privilege purposes and that although a party anticipating possible prosecution will often need to make further investigations before it can say with certainty that proceedings are likely, that uncertainty does not in itself prevent proceedings being in reasonable contemplation. The fact that ENRC did not have the information required to evaluate the whistleblower email, therefore causing it to be uncertain as to whether a crime had in fact taken place, was not a bar to having the protection of litigation privilege. The Court opined that it would be wrong to deny a potential defendant the benefit of litigation privilege when asking his or her lawyer to investigate the circumstances of the alleged offence. It concluded that ENRC did contemplate that prosecution was possible when the documents in question were created and, therefore, these documents were protected by litigation privilege.

The Court of Appeal decision went some way to restoring the status quo in relation to privilege but much of the reasoning in the case is highly fact-specific; the judgment should not be interpreted to extend litigation privilege to all documents created in all internal investigations. Many pitfalls remain, with challenges by opponents and regulators and privilege issues continuing to trouble businesses, their lawyers and the courts. Although some cases have confirmed the status of legal professional privilege as a fundamental right, there are no guarantees that any document created during an internal investigation will be legally privileged. Nevertheless, steps can be taken to maximise the chance of succeeding with such a claim, such as:

- involving lawyers (whether external or in-house) as soon possible;
- marking all communications pertaining to legal advice as 'privileged and confidential';
- segregating privileged and non-privileged documents;
- refraining from forwarding or creating new documents that summarise the legal advice received;
- encouraging employees not to amend or quote extracts from legal advice; and

© Law Business Research 2021

- if there is the reasonable possibility of potential litigation at a later stage, recording this in writing, and giving as much detail as possible, to evidence any subsequent legitimate claim for litigation privilege.

Parties are able to obtain legal advice in the context of an internal investigation, and confidential communications between a lawyer and a client, provided they are for the dominant purpose of seeking or giving legal advice, are likely to be privileged under legal advice privilege principles. These principles generally do not protect communications involving third parties. However, the Court of Appeal in *ENRC,* as well as courts in some subsequent cases, have expressly left open a question as to whether aspects of current UK law on legal advice privilege should be reviewed at a later date by the UK Supreme Court. It is likely, therefore, that the subject of privilege in internal investigations will be a matter of continuing development of UK law.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There are two main forms of legal professional privilege:

- legal advice privilege, which protects confidential communications (and evidence of those communications) between a lawyer and a client (but not communications with third parties), provided that the communications are for the dominant purpose of seeking and receiving legal advice; and
- litigation privilege, which protects confidential communications (and evidence of those communications) between a lawyer and a client or third party, or both, or between a client and a third party, created for the sole or dominant purpose of obtaining information or advice in connection with the conduct of existing or reasonably contemplated litigation (including avoiding or settling, as well as defending or resisting, that litigation).

The holder of the privilege is the client and survives the death or dissolution of the client (*Addlesee v. Dentons* [2019] EWCA Civ 1600).

In the case of corporate investigations, the client tends to be represented by the group of individual employees or directors charged with seeking and receiving legal advice on behalf of the company (or commissioning or conducting the internal investigation) rather than the entire corporate entity. This group of individuals usually includes the in-house legal team and some or all of the board of directors or a subcommittee established by a company, but this group should be defined as soon as any external lawyers are engaged or at the outset of an investigation. This helps to ensure that there is a defined group from whom instructions by lawyers can be received and to whom advice is provided, which safeguards any claim of legal advice privilege.

© Law Business Research 2021

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, although not in the context of an antitrust and competition investigation by the European Commission. This exception may well also apply to other EU investigations, such as state aid and merger control. Consequently, where competition matters and other matters in which EU bodies might get involved at a later stage are concerned, it is best to involve external counsel. In-house counsel must always be careful to ensure that they distinguish between legal advice and advice that is commercial in nature, since the latter will not attract legal professional privilege.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Advice sought from foreign lawyers in investigations in the United Kingdom is subject to the same legal professional privilege as advice sought from lawyers within the United Kingdom. The UK courts will apply UK law on privilege to determine the extent to which privilege applies. If a document satisfies the test for legal advice privilege or litigation privilege under UK law, the document will be treated as privileged. This decision is made regardless of whether that document would not have been privileged under a foreign law.

This principle can have the opposite effect in respect of any documents that would be privileged under foreign law but do not meet the requirements for privilege under UK law. The foreign privileged documents would not attract legal professional privilege in the United Kingdom.

Privilege can attach to the advice given by foreign lawyers (including in-house lawyers), provided they are acting in their professional capacity in connection with the provision of legal advice. The 2020 case of *Tatneft v Bogolyubov and others* ([2020] EWHC 2437) clarified that the communications of foreign lawyers who are 'acting in the capacity or function of a lawyer' are protected by legal professional privilege.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

UK authorities have frequently stated that they have no interest in communications between a client and its lawyers as to questions of liability or rights; however, in recent years, law enforcement agencies, such as the SFO, have challenged assertions of legal professional privilege over factual aspects of internal investigations and have expected the waiver of claimed legal professional privilege in the event of any self-report. The authorities have stated previously that a refusal to waive a well-made-out claim of legal professional privilege will not be held against a company, but a waiver of such a claim would be good evidence of co-operation. False or exaggerated claims of legal professional privilege will continue to be considered strong evidence of not co-operating and will be challenged. The 2018 *ENRC* Court of Appeal judgment has confirmed that even when a party may lead the SFO to believe that it might in future waive privilege over certain documents, this does not in itself amount to a waiver of privilege and would only amount to such a waiver in the event of a formal agreement.

© Law Business Research 2021

In 2019, the SFO issued guidance on its requirements for corporate co-operation in relation to its investigations. The guidance provides that 'if the organisation claims privilege, it will be expected to provide certification by independent counsel that the material in question is privileged'.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is a concept of limited waiver of legal professional privilege, and it is for the individual or entity waiving the privilege to determine the extent of the waiver.

It is important to be very clear as to the scope of the waiver with regard to the purpose for which the privileged information can be used and with whom it can be shared, particularly if a party seeks to prevent the information being shared with other domestic or foreign enforcement authorities or parties in any related civil proceedings. Generally, there are various gateways where evidence is shared between law enforcement agencies in the United Kingdom (and sometimes elsewhere), and proposals for a limited waiver from a corporate may not be acceptable to a law enforcement agency given the wider duties of disclosure or information sharing.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This will depend on a number of factors, including the terms of the waiver, the circumstances in which the material was received by the UK authority, and whether the UK authority disputes the claim of privilege, for example, if the UK authority asserts that the material falls within the crime-fraud exception.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists in most parts of the United Kingdom (opinions are divided as to its existence in Scotland) and can be used to preserve privilege in documents disclosed to third parties who have, at the time of the disclosure, a common interest in the subject matter of the privileged document or the litigation for which the document was created.

It is advisable when disclosing information under the common interest privilege to ensure that the recipient understands that the document has been disclosed on this basis and to obtain undertakings from the recipient that the privilege will not be waived. Typically, in criminal-related investigations, common interest privilege has very limited practical scope, because it is often in doubt whether two parties do, in fact, have a common interest.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

Privilege can be claimed over confidential communications (and evidence of those communications) between a lawyer and a client or third party, or both, or between a client

© Law Business Research 2021

and a third party, created for the sole or dominant purpose of obtaining information or advice in connection with the conduct of existing or reasonably contemplated litigation (including avoiding or settling, as well as defending or resisting, that litigation).

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

An internal investigation is a fact-finding exercise and interviews will often be considered material to any internal investigation. However, it is advisable always to be sensitive to the expectations of investigating authorities, to avoid any criticism that interviews could have prejudiced the law enforcement investigation.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

In its ENRC judgment, the Court of Appeal held that, on the facts of that case, factual notes of what is said by a witness to a lawyer constituted a privileged document.

It should also be borne in mind that when proceedings are not in contemplation, communications between interviewees and counsel not made in the course of giving instructions to counsel will not attract litigation privilege or legal advice privilege. Only communications between counsel and those entrusted by the company to give instructions to counsel will attract legal advice privilege.

In summer 2019, the Serious Fraud Office (SFO) issued guidance on its requirements for a company to be considered to be adopting a co-operative approach with the SFO, which includes guidance on witness interviews. The Law Society's position is that no client should be put under pressure to waive privilege or conduct affairs in such a way that properly construed privilege does not apply.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Although there are no general, formal requirements when conducting witness interviews as part of an internal investigation, best practice dictates that, irrespective of whether the interviewee is an employee or a third party, they should be informed:

- that the interview is part of a fact-finding exercise and, if applicable, in contemplation of litigation;
- if they are implicated in any wrongdoing;
- that the lawyer conducting the interview represents the company and not the interviewee;
- that the interview notes created by the lawyer belong to the company and, therefore, any privilege in the notes rests with the company;
- the company may choose to provide the notes to an authority (and this is at its election); and

© Law Business Research 2021

- that the interview is confidential and the contents of the interview should not be discussed with other employees or witnesses (to avoid contaminating their recollection and generally to protect the integrity of the process).

Care should also be taken not to taint a witness's recollection, for example by disclosing previously unseen material or discussing another witness's statement.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

It is becoming more common for interviewees to be legally represented in initial fact-finding interviews during internal investigations, and companies should not refuse a request from an individual to be legally represented at his or her own expense. When employees may incriminate themselves during an interview, there are compelling ethical reasons why a company may suggest that an employee may wish to obtain his or her own independent legal advice.

Documents can be put to the interviewee. A copy of each of the documents referred to, or an interview pack, should be retained as part of the record of the interview, as a matter of good internal investigation practice.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Section 330 of the Proceeds of Crime Act 2002 (POCA) places a specific duty on employees of regulated businesses (i.e., financial services firms and professional services such as lawyers and accountants) to make a report to the National Crime Agency (NCA) when they have reasonable grounds to know or suspect that another person is engaged in money laundering and that knowledge or suspicion came to them within the course of their regulated business. Failure to make a report in those circumstances carries a risk of imprisonment or a fine, or both, for individuals (and fines for companies), unless, in the case of individuals, they have reported to their company's money laundering reporting officer (MLRO). Other similar offences arise under section 331 of POCA regarding MLROs who have failed to report to the NCA, given their designated statutory duties to do so.

In June 2021, the Crown Prosecution Service (CPS) published its revised legal guidance on section 330 of POCA confirming that the CPS will consider prosecuting for a failure to report money laundering suspicions even though there is insufficient evidence to establish a predicate money laundering offence. This represents a significant policy shift as, prior to the guidance update, the CPS did not charge under section 330 if there was insufficient evidence to establish that money laundering was planned or undertaken.

Any company (regulated or non-regulated) may make a report to the NCA if it has a suspicion that it possesses funds obtained as a result of suspected criminal conduct by the company or its employees, as this may be a money laundering offence under POCA,

© Law Business Research 2021

or terrorist financing (under part 3 of the Terrorism Act 2000). In addition, when a company (regulated or non-regulated) knows or suspects that property it intends to deal with is criminal (i.e., it constitutes or represents, in whole or part, directly or indirectly, the benefit of a person's criminal conduct), it should make a Defence Against Money Laundering report (DAML) to the NCA. Note that the DAML only applies to future actions and cannot cure past breaches. In both cases, a report to the NCA of any of these types of suspicions and activities can provide a statutory defence to money laundering if made as soon as practicable.

A money laundering report to the NCA is not a self-report for the purposes of a deferred prosecution agreement (DPA) or mitigation of sentence. A self-report must be made directly to the relevant authority, such as the Serious Fraud Office (SFO).

Note also that the Fifth Money Laundering Directive (EU) 2018/843, which came into force on 10 January 2020, expands the scope of businesses to which the UK's anti-money laundering regime applies (for example, to tax advisers, letting agents and crypto-asset exchanges), as well as amending a number of the substantive requirements. In Scotland, there is an obligation to report any knowledge or suspicion of serious organised crime to the police when this knowledge or suspicion originates from information obtained in the course of business or as a result of a close personal relationship (Criminal Justice and Licensing (Scotland) Act 2010). In Northern Ireland, additional reporting duties apply under the Criminal Law (Northern Ireland) Act 1967.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The question of when and whether to self-report has been the subject of considerable debate following the *Rolls-Royce* case, which involved a DPA (notwithstanding that there was no self-report) and the *Airbus SE* case, respectively.

Prior to the DPA agreed in *Rolls-Royce* in January 2017, it was considered advisable for a company to self-report if it wished a matter to be settled by way of a DPA; the SFO had articulated that one of the preconditions of a DPA was a genuinely proactive approach by the company, including a full self-report (i.e., complete disclosure of the facts).

However, doubt was cast on whether a self-report was a precondition to a DPA in light of the DPA secured by Rolls-Royce in circumstances that did not follow a self-report. The SFO, and indeed the court in approving the DPA, emphasised that the circumstances in which Rolls-Royce secured a DPA (notwithstanding that it had not self-reported) were due to the extraordinary level of co-operation with the SFO that followed once the offending conduct was already known in part to law enforcement authorities.

In respect of Airbus SE, the commercial and defence and space divisions were charged with five counts of failure to prevent bribery. The conduct covered by the UK DPA took place across Sri Lanka, Malaysia, Indonesia, Taiwan and Ghana, between 2011 and 2015. In its judgment, the court remarked that the seriousness of the criminality in this case was grave, with worldwide conduct that took place over many years. It also noted that once the

© Law Business Research 2021

wrongdoing was identified, Airbus SE overhauled its compliance, which resulted in the company putting in place the following remedial steps:

- redesigning its compliance structure and oversight mechanisms;
- rolling out improved and strengthened due diligence processes;
- launching a required company-wide anti-bribery and corruption risk assessment;
- bringing in a newly elected management team; and
- launching internal investigations into the actions of existing and former employees.

When approving the DPA, the court cited these extensive steps, recognising that the overhaul to the management and compliance structure of the business left it 'a changed company to that which existed when the wrongdoing occurred'. This contributed to a 50 per cent reduction in the financial penalty imposed by the DPA.

The SFO has now issued guidance on what it considers amounts to co-operation with its investigations, including a requirement to report a suspected fraud or bribery within a reasonable time of the suspicion arising. The guidance makes it clear that co-operation will be a relevant factor in making charging decisions (i.e., whether to prosecute, recommend a DPA or take no further action). There is no presumption that self-reporting will lead to no further action.

The SFO does not publish details of the self-reports that have led to no further action. Whether a DPA will be available in the absence of a self-report in future remains to be seen.

To date, the SFO has not secured the successful conviction of any of the individuals who have been prosecuted in connection with previous DPAs, including those with Tesco Stores Limited, Güralp Systems Ltd and, most recently, Serco. Commentators have pointed to the different considerations for a corporate and the SFO to reach agreement on the factual basis of a DPA compared with the separate evidential issues for the SFO in bringing criminal proceedings against any individuals that may arise following a DPA.

Note that DPAs are only available to corporate defendants and not to the individual employees or directors involved in the criminal conduct.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

Before making a self-report, companies and their advisers are likely to consider the level of investigation that is appropriate to ascertain the extent and nature of the potential offending, balancing this against a risk that any delay in reporting will face criticism and could jeopardise co-operation credit with law enforcement agencies at a later stage.

UK authorities have advised that for a company to be afforded full credit for making a self-report, it must be made within the context of a genuinely proactive and co-operative approach by the company.

The SFO's outline of the process to be adopted by corporate bodies or their advisers when self-reporting provides that:

- initial contact, and all subsequent communication, must be made through the SFO's intelligence unit, using the secure reporting form;
- hard copy reports setting out the nature and scope of any internal investigation must be provided to the SFO's intelligence unit;

© Law Business Research 2021

- all supporting evidence, including, but not limited to, emails, banking evidence and witness accounts, must be provided to the SFO's intelligence unit; and
- further supporting evidence may be provided during the course of any current internal investigation.

In Scotland, the Crown Office and Procurator Fiscal Service's self-reporting initiative, which applies in relation to corporate bribery offences, requires a written report to be submitted on the company's behalf by a solicitor.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is both possible and desirable to enter into a dialogue with the relevant authority before or on receipt of a notice or warrant to discuss any concerns the company has, for example that the deadline for compliance is unreasonable, or the description of the information and documents requested is unclear.

With regard to search warrants served on businesses, the police do not usually contact a business to discuss the terms of a warrant prior to turning up and executing the warrant. However, depending on the circumstances, the police may be willing to discuss the implementation of the warrant to avoid unnecessary disruption to the business's legitimate activities and the risk of the warrant being challenged.

Materials subject to legal professional privilege may be withheld when responding to a search warrant. Warrants often do not address how privileged materials should be handled, and dealing with issues of privilege tends to be a matter for negotiation. The lawyer for the company should object to privileged materials being reviewed or seized and offer to set aside potentially privileged materials for subsequent review by the company's legal agent. If the authority will not agree to this course, it may be proposed to appoint independent counsel (usually an advocate, barrister or solicitor) to review potentially privileged material and to make an initial determination as to whether or not the material is, in fact, privileged. If the authority will not agree to proceed on that basis, counsel for the company should insist that any privileged material should be sealed, unread and delivered to the court to enable it to adjudicate on the matter. In the event that such suggestions are not acted on by the authority, the company may need to seek to overturn the warrant by presenting to the court a judicial review (or a bill of suspension in Scotland).

55 Are ongoing authority investigations subject to challenge before the courts?

The exercise of powers by any public authority, such as in undertaking an investigation, can be challenged by application to the court for a judicial review (a bill of suspension in Scotland) if considered to be unlawful.

© Law Business Research 2021

If found to be unlawful, the court can order various remedies, such as stopping the exercise of that power, rendering it ineffective, or awarding damages.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

While attempting to deal with notices or court orders issued by various jurisdictions as one consistent disclosure package would reduce effort and costs, it is generally advisable to deal with them separately but have protocols in place to ensure consistent approaches are maintained to any relevant documents to be produced. Court orders and notices issued under compulsory powers usually negate data protection laws and any obligations of confidentiality to third parties. Consequently, civil proceedings cannot be brought by third parties against a company for its actions in providing material in response to a lawful court order or compulsory notice as long as the material provided was within the scope of the notice or order. However, if the company voluntarily provides material beyond the scope of the notice or order, and in doing so breaches a confidentiality obligation or data protection law, it could expose itself to claims.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, if information is in the control of a company (e.g., a parent company with a right to take possession, inspect or take copies of a subsidiary's documents), the company will be expected, and may be required, to search for and produce all requested material, even when it is located in another country. In practice, if a company wishes to seek credit for co-operation, it should comply with any reasonable requests, whether or not it is required to.

The exception is when the data protection legislation in the other country does not permit the removal or transfer of the data from that jurisdiction. In those cases, the requesting authority will generally need to use mutual legal assistance to obtain the material through foreign counterparts.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The UK authorities can and do share information and investigative materials with authorities in various other countries (for intelligence purposes and the detection and prevention of crime), whether or not there is a mutual legal assistance agreement with that country. This occurs regardless of whether the country is providing information or materials in return, although reciprocity is generally expected.

© Law Business Research 2021

Where material is required for a prosecution, a mutual legal assistance request must be made. UK law authorities will only provide assistance that conforms with the UK's laws and international obligations.

A list of the international mutual legal assistance and extradition agreements to which the UK is a party can be found on the UK government website (https://www.gov.uk/guidance/mutual-legal-assistance-mla-requests). Having left the European Union, the United Kingdom will now have to request assistance from EU Member States (and vice versa) using channels provided for under the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its protocols, as supplemented by the EU–UK Trade and Cooperation agreement.

The UK authorities can provide further assistance by conducting dawn raids in the United Kingdom on the foreign authority's behalf, interviewing witnesses or suspects, freezing assets, or arresting and extraditing suspects.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Law enforcement authorities have a general duty not to disclose information or material received during the course of an investigation, and which is not otherwise in the public domain, unless the public interest in the disclosure outweighs the private interests of the owner. Furthermore, before disclosing information to a third party, the law enforcement agency should provide the owner with sufficient notice of the request to allow an opportunity for objections to the disclosure (*Marcel and Others v. Commissioner of Police of the Metropolis and Others* [1992] 2 WLR 50). Any objections should be considered and advance notice should be provided of an intention to disclose regardless. Notice does not have to be given when it would be inappropriate or impracticable to provide notice, for example if it would prejudice an investigation by the law enforcement agency requesting the information (*R (on the application of Kent Pharmaceuticals Ltd) v. Serious Fraud Office and another* [2005] 1 W.L.R. 1302). The police can also retain property after the Crown Prosecution Service decides not to prosecute, if a private prosecution is being contemplated or is taking place (*Scopelight Ltd v. Chief Constable of Northumbria* [2009] EWCA Civ 1156; [2010] 1 Cr. App. R. 19).

Section 3 of the Criminal Justice Act 1987 further limits disclosure by the Serious Fraud Office (SFO) to third parties. Information obtained during the course of an investigation by the SFO can only be disclosed to certain specific government departments or bodies, or competent authorities specified in the Act, and only for the purposes of any criminal investigation or criminal proceedings, whether in the United Kingdom or abroad and for the purposes of assisting any public or other authority under the order. The list of competent authorities is comprehensive and includes any entity with supervisory, regulatory or disciplinary functions; however, it does not include liquidators, provisional liquidators, administrators or administrative receivers.

Section 18 of the Commissioners for Revenue and Customs Act 2005 contains an additional statutory duty of confidentiality that criminalises the wrongful disclosure of information about, acquired as a result of, or held in connection with a function of Her

© Law Business Research 2021

Majesty's Revenue and Customs (HMRC). Disclosures made by HMRC will therefore be made in accordance with specific statutory gateways, such as section 19 of the Anti-terrorism, Crime and Security Act.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In these circumstances, the company should not provide the documents, but should inform the requesting authority of the reason why these documents cannot be provided (i.e., that the data protection laws in the other country constitute reasonable excuse for lack of compliance).

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

The collection and use of personal data are governed by the Data Protection Act 2018 (the DP Act), including restrictions on the disclosure of personal data. Personal data is defined as data that relates to a living individual who can be identified from that data. The data protection principles set out how personal data should be processed, which include that it should be fairly and lawfully processed as well as only processed as far as is necessary. The DP Act also gives certain rights to the data subjects. In practice, this can mean that unless certain conditions are achieved, personal data should not be transferred. However this is subject to certain relaxations if the material is requested by a notice or court order issued on the grounds that the material is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of any tax or duty, or of any imposition of a similar nature.

In *Elgizouli v. Secretary of State for the Home Department* [2020] UKSC 10, the United States had made a mutual legal assistance request to the United Kingdom. The Home Secretary requested that the information would not be used in a prosecution in which the death penalty would be the resultant sentence. This assurance could not be given but the information was provided in any event. The UK Supreme Court determined that the decision had been unlawful under the DP Act.

The term 'blocking statute' is generally not applicable except in the field of financial and trade sanctions, for which there is blocking legislation in relation to specific US sections that have extraterritorial application.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

When material is provided voluntarily and without restrictions, the authority is free to share it with third parties or other authorities, and to use it for any purpose.

In general, it is advisable only to provide material voluntarily having obtained contractual undertakings that agree the restricted basis on which the material has been provided

© Law Business Research 2021

(e.g., only for use by that authority in the course of an investigation and not to be shared with other parties).

Although contractual undertakings restrict an authority's ability to voluntarily provide material to other parties, they do not prevent third parties from obtaining court orders against the authority requiring production of the material. However, production orders should only be granted when it is in the interests of justice, and the fact that the material came into the possession of the authority under the restrictions imposed by the undertakings may lead a court to determine that it is not appropriate to grant a production order against the authority in that context, particularly as the third party could attempt to obtain the documents from an unfettered source, such as the company.

In general, authorities are restricted as to how they can share material they obtain as a result of exercising their compulsory powers or court orders, and customarily such material should only be shared when it is necessary for an investigation and the disclosure is proportionate.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Penalties on conviction include imprisonment for individuals, fines, compensation and confiscation orders. Individuals can also be disqualified from being a director of a company for up to 15 years. Monitoring may be imposed as part of a deferred prosecution agreement.

Companies convicted of certain offences, including active bribery and money laundering, must also be debarred from public tendering for up to five years.

Regulatory authorities can impose additional penalties. For example, the Financial Conduct Authority can withdraw a firm's authorisation and prohibit it from undertaking specific regulated activities for up to 12 months, prohibit individuals from carrying out regulated activities, or impose fines on firms or individuals. The Prudential Regulation Authority (which is responsible for the prudential regulation and supervision of around 1,700 banks and other firms) can restrict a firm's permission to conduct regulated activities or impose a fine. Her Majesty's Revenue and Customs can also consider the imposition of restrictions in respect of regulation or licensing regimes for matters under its control.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The Public Sector Procurement Directive (2014/24/EU) was transposed into UK law by the Public Contracts Regulations 2015 (the 2015 Regulations). Under these Regulations, a company must be excluded from public procurement if it has been convicted in the past five years of any offences from a list that includes conspiracy, corruption, bribery, money laundering and fraud. The corporate offence of failure to prevent bribery (Bribery Act 2010, section 7) is not included in this list of offences for mandatory debarment (although a conviction could lead to discretionary debarment).

© Law Business Research 2021

The 2015 Regulations also provide a list of offences that carry discretionary debarment for up to three years, including professional misconduct, non-payment of tax and distortion of competition.

The 2015 Regulations allow companies to recover eligibility to bid for public contracts following a debarment by demonstrating evidence of self-cleaning, such as the payment of compensation to the victim of the offending, clarification of the facts and circumstances of the offence in a comprehensive manner, co-operation with the investigating authority, and the implementation of appropriate measures to prevent further criminal offences or misconduct.

65 What do the authorities in your country take into account when fixing penalties?

When fixing penalties following conviction, courts must have regard to the sentencing guidelines published by the Sentencing Councils for England and Wales and Scotland. Similarly, in Northern Ireland, sentencing guidelines are issued by the Lady Chief Justice's Office.

Specific sentencing guidelines were published in 2014 for England and Wales (not Northern Ireland) in respect of corporate fraud, bribery and money laundering offences providing that, when sentencing a company, the court must first determine whether compensation or confiscation orders should be made. Thereafter, the court should consider, inter alia, the following issues:

- the level of culpability and financial harm;
- any aggravating or mitigating factors, for example whether the criminal activity was endemic or whether the corporate offered full co-operation with the law enforcement authority during the investigation;
- the financial circumstances of the company; and
- the stage at which a guilty plea was entered (if the matter was not contested).

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Deferred prosecution agreements (DPAs) have been available in England and Wales (as a result of the Crime and Courts Act 2013) since 2014 as an alternative disposal for corporate offending. DPAs are not currently available in Scotland, where a civil settlement regime applies, or in Northern Ireland. Non-prosecution agreements do not exist in the United Kingdom, although Her Majesty's Revenue and Customs (HMRC) applies a published selective prosecution policy and so, in a range of situations, may pursue suspected wrongdoing by means of its civil powers, most specifically by the use of the 'contractual disclosure facility', which affords immunity from criminal action if full material disclosure is made within a civil enquiry and settlement into an individual (rather than body corporate).

The Serious Fraud Office (SFO) and Crown Prosecution Service (CPS) have published a Code of Practice explaining the DPA process (the CPS rather than HMRC

© Law Business Research 2021

will determine the merits of seeking to agree a DPA in respect of domestic tax facilitation prosecutions). The SFO issued guidance in summer 2019 setting out factors amounting to co-operation with its investigations and, in October 2020, published a chapter from its handbook adding to the transparency around how it engages with companies when a DPA is in prospect.

A prosecutor may invite, at its discretion, a corporate suspect into DPA negotiations if it determines that having identified the full extent of the offending, the evidential test has been satisfied and the public interest would benefit from a DPA. Until the *Rolls-Royce* case, the orthodox view was that a corporate will only be invited to negotiations when a self-report has been made and the corporate has fully co-operated with the authority. Following *Rolls-Royce*, it is possible that a DPA may be negotiated in wider circumstances, including when there has been no self-report but subsequent extraordinary co-operation by a corporate with the law enforcement authority.

If it is possible to agree the terms of a DPA and a statement of facts, the corporate will be formally charged with the criminal offence or offences and the matter will be brought before a judge for approval. The judge will only approve the DPA if satisfied that it is in the interests of justice and the terms are fair, reasonable and proportionate. The judge can adjourn the matter to obtain further information or clarification as to the facts or terms.

If judicial approval is given, the criminal proceedings will be suspended for a set period as defined by the terms of the DPA. The terms and facts of the DPA will then be published on the authority's website.

If the corporate complies with the terms of the DPA, the criminal proceedings will be formally discontinued at the conclusion of the set period. If the corporate breaches the terms and the breach cannot be remedied, the criminal proceedings will resume.

To date, 12 DPAs have been agreed in the United Kingdom.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Reporting restrictions can be placed on DPAs while criminal proceedings against connected individuals are under way. Reporting restrictions were imposed on the *Sarclad* and *Tesco* DPAs because of ongoing proceedings against the individuals allegedly responsible for the misconduct. Following the conclusion of those proceedings, the reporting restrictions were lifted. Reporting restrictions currently apply to the two most recent DPAs entered into by 'two unnamed companies' following their judicial approval on 19 July 2021.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before entering into a settlement with a law enforcement authority, a company should assess the merits and strength of the prosecution and defence cases, the likelihood of conviction, the expected time, cost, reputational damage and other adverse effects of

© Law Business Research 2021

a lengthy investigation and trial, and the likely penalties in the event of a conviction, including possible debarment from public procurement tenders.

The company should then carefully assess the terms of the proposed settlement, including the effect that continuing co-operation could have on the business (legal costs, staff resources, etc.); whether the settlement will resolve the matter in all relevant jurisdictions and, if not, the effect the settlement could have in regard to ongoing investigations in other jurisdictions (e.g., whether the authority that has settled will disclose information and assist foreign authorities); and any other adverse effects that the settlement could have on the future of the business.

Ultimately the company should balance the seriousness of the charge and the potential consequences of a conviction (including whether it results in debarment) against the terms of the settlement, as in some circumstances the terms of a settlement, including, for example, the costs of regular review and monitoring by an independent monitor (typically a large accountancy or law firm), could be more disadvantageous to a company than a conviction.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The Crime and Courts Act 2013 and the related guidance permit the appointment of monitors in appropriate cases. The Deferred Prosecution Agreements Code of Practice (the DPA Code) sets out the roles, duties and mechanics of appointing monitors as a term of a DPA. The Code of Practice stops short of requiring the appointment of a monitor as a condition of a DPA. The *G4S C&J* DPA agreed in July 2020 was the first that required an SFO-approved independent monitor to report on the organisation's compliance improvements over the DPA's three-year duration.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel private civil actions are allowed. Generally, but not always, the criminal proceedings will take precedence and civil proceedings can be stayed for the duration of the criminal investigation, so as not to prejudice any criminal proceedings.

Private claimants will only gain access to specified information in the authority's files if they obtain a court order. Before making any such order, the court would carefully consider the reason why the private claimant requires the information, whether the claimant would be able to obtain the information from any other source, the method by which the authority obtained the relevant information, for example if it was obtained under compulsory powers, and whether the information is likely to contain any confidential, privileged or personal information relating to third parties.

Increasingly, small numbers of private criminal prosecutions involving allegations of fraud are being conducted in the courts of England and Wales. The instigation of a private prosecution is provided for in section 6 of the Prosecution of Offences Act 1985 and is subject to a power of the Director of Public Prosecutions to take over the private prosecution at any stage (and, if the Director chooses, to discontinue it).

© Law Business Research 2021

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

It is a contempt of court to publish a report, including via social media posts, that creates a substantial risk that the course of justice in active criminal proceedings will be seriously impeded or prejudiced. Proceedings are active for this purpose after arrest or charge and until the proceedings have been concluded, for example by acquittal or conviction, or discontinuance by the authority. As a result, there is generally very little substantive media reporting of criminal investigations until the end of a trial, other than to state the facts of arrests and report court hearings.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common practice for companies to hire a public relations (PR) firm to manage a large-scale corporate crisis to mitigate potential reputational damage. It is important to ensure a consistent approach by opening good lines of communication between the company's internal marketing team and the external PR firm, and to ensure that the PR firm is aware of any legal or corporate issues (including any agreements reached with the investigating authority with regard to press releases, etc.).

It is also vitally important that public statements do not have the potential effect of prejudicing ongoing criminal proceedings (for example, the trial of the company or individual employees) or contradict any defence on which the company may later seek to rely. For those reasons, statements issued by a company under investigation should be brief and factual, and should always be approved by the company's criminal law advisers.

73 How is publicity managed when there are ongoing related proceedings?

It is vitally important that public statements issued by the company do not have the potential effect of prejudicing ongoing criminal proceedings, such as the related prosecution of employees or third parties.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under the UK Listing Rules, publicly listed companies must issue a market announcement without delay regarding any major new development that may affect their business, if the development may lead to a material movement in the companies' listed securities (including shares and bonds). The point at which a company is informed that it is the subject of an investigation would generally require an announcement, as would the settlement of criminal proceedings.

If the matter is to be settled by way of a deferred prosecution agreement, the matter is not settled until it has actually been approved by a judge at a court hearing. In practice,

© Law Business Research 2021

prior to the final hearing (at which the parties will generally expect approval to be given, as the terms, among other things, will have been examined and challenged at preliminary hearings), the company and the authority will have agreed press statements to be released to the market and wider public as soon as approval is given.

Similarly, under the Alternative Investment Market Rules (AIM is a sub-market of the London Stock Exchange), an AIM company is required to update its nominated adviser (Nomad) of any developments that may affect the business if that development may lead to a significant price movement of its securities. The Nomad is responsible to the London Stock Exchange for advising the AIM-listed company on its responsibilities regarding its admission to AIM and continuing obligations to the market. With the assistance of the Nomad, an AIM company is required to issue notifications of any developments to the market without delay.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

ESG issues are becoming increasingly important parts of the corporate agenda. Organisations are subject to a number of mandatory reporting requirements on ESG issues and many companies choose to adhere to voluntary reporting frameworks and initiatives. There is no single piece of ESG legislation setting out specific obligations to which UK organisations must adhere, but rather an array of legislation on equality and diversity, protection of employees, health and safety, protection of the consumer, environmental protection and human rights. Some examples of this legislation are as follows:

- Companies Act 2006, section 172 requires that a director 'act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole', having regard to a number of statutory factors such as the likely consequences of any decision in the long term, the interests of the company's employees and the company's business relationships with suppliers, customers and others. Large companies are required to report on this by way of a 'section 172 statement' describing how the directors have had regard to employees and other interests when performing their duty.
- Companies Act 2006, section 415 requires all companies (other than small companies) to prepare a strategic report for each financial year as part of their annual report. The report must include, to the extent necessary to understand the development, performance or position of a company's business, analysis using key performance indicators (KPIs), including information on environmental matters. The government's Environmental Reporting Guidelines identify six environmental KPIs, namely greenhouse gases, water, waste, resource efficiency and materials, biodiversity and ecosystem services, and emissions to air, land and water. Additional requirements apply to quoted companies.
- The Companies, Partnerships and Groups (Accounts and Non-Financial Reporting) Regulations (SI 2016/1245) implemented aspects of the Non-financial Reporting Directive 2014/95/EU, as regards disclosure of non-financial and diversity information by certain large undertakings and groups.

© Law Business Research 2021

- The Companies (Miscellaneous Reporting) Regulations 2018 (SI 2018/860) introduced new reporting requirements in relation to engagement with employees, and engagement with suppliers, customers and other stakeholders, in addition to the requirement for a 'section 172 statement'. These reporting requirements apply to financial years beginning on or after 1 January 2019.
- The Modern Slavery Act 2015 requires certain commercial organisations to produce and publish a slavery and human trafficking statement for each financial year. The statement must set out what steps have been taken during the financial year to ensure that modern slavery is not occurring in supply chains or within the organisation.
- The Companies (Directors' Report) and Limited Liability Partnerships (Energy and Carbon Report) Regulations 2018 supplement narrative reporting requirements on greenhouse gas emissions and other environmental effects in annual corporate reports under the Companies Act 2006. The Regulations require additional reporting on emissions, energy consumption and energy efficiency action by quoted companies, large unquoted companies and large limited liability partnerships.

In addition to annual corporate reporting on environmental matters, certain environmental regimes also require businesses to report environmental information to the relevant regulator, and the regulators maintain public registers of environmental information about, for example, environmental consents, breaches and enforcement action.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

In November 2020, the UK government published a road map towards mandatory climate-related disclosures across all sectors of the economy aligned with the recommendations of the Taskforce on Climate-related Financial Disclosures (TCFD). The government announced its intention to make TCFD-aligned disclosures mandatory across the economy by 2025, with a significant portion of mandatory requirements in place by 2023. The UK Taskforce's Interim Report, and accompanying road map, sets out an indicative pathway to achieving that ambition.

The road map set a timetable for cross-sector full disclosure reporting on the following:

- pension schemes of over £5 billion, banks, insurance companies and building societies will be expected to comply with TCFD recommendations. Furthermore, UK premium listed companies (for financial years starting on 1 January 2021 onwards) must disclose whether their disclosures are consistent with the recommendations of the TCFD and, if not, explain why and provide a description of steps towards future compliance;
- smaller pension schemes, asset managers and life insurers will be subject to disclosure requirements from 2022;
- life insurers, pension providers regulated by the Financial Conduct Authority (FCA) and other UK-authorised asset managers will be subject to disclosure requirements from 2023;
- all other occupational pensions schemes and UK financial services firms will be subject to mandatory climate-related financial disclosures by 2025; and
- implementation of a UK green taxonomy (based on the EU taxonomy).

© Law Business Research 2021

The government will provide an update on progress in the 2022 refresh of the Green Finance Strategy.

It is anticipated that the oversight structure relating to the above will probably require refinement as each of the above steps is embedded. At present, the FCA, the Prudential Regulation Authority, the Department for Work and Pensions and the Department for Business, Energy and Industrial Strategy all share some level of oversight.

A draft Environment Bill includes provisions intended to prevent illegal deforestation by placing controls on the supply chain. These would apply to large businesses with a turnover greater than a set threshold and would prohibit those companies from using a 'forest risk commodity' or a product derived from such a commodity in their UK activities unless relevant local laws relating to that commodity had been complied with. It would also require them to establish and maintain a due diligence process for the use of any such products and to report on due diligence undertaken annually.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

The growth of the body of legislation and regulatory guidance in this area has certainly accelerated, and it is anticipated that it will be accompanied by a corresponding rise in litigation relating to the core areas of ESG.

Financial regulators are making it increasingly clear that they will take action against firms that mislead the public about the climate credentials of their products. On 19 July 2021, the FCA published a letter to the chairs of authorised fund managers setting out regulatory expectations on the design, delivery and disclosure of ESG and sustainable investment funds. The letter emphasised the FCA's principles for ensuring that any ESG-related claims are clear and not misleading, both at the time of application and on an ongoing basis, enabling consumers to make informed choices. The letter followed the FCA's detailed report on the effects of presenting funds as 'sustainable' on consumer investment decisions (and associated mis-selling risks). Mis-selling of 'green' products, for example through misrepresenting ESG ratings or misleading customers as to a fund's exposure to investments with positive and negative ESG effects, will probably give rise to increasing regulatory scrutiny and consumer claims, whether by way of regulatory interventions (including enhanced supervisory requirements and enforcement actions), litigation or via the Financial Ombudsman Service. The FCA's current regulatory framework – and proposed changes specifically aimed at ESG products – will be fundamental in this.

In February 2021, the Serious Fraud Office charged a biodiesel trader with fraud and money laundering in connection with its investigation concerning the sustainable fuel sector. Although not an example of ESG-related enforcement, it is an example of how financial crime cases have arisen from sectors that may have a ESG or related focus.

© Law Business Research 2021

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

On 4 November 2020, the government published the outcome of its call for evidence in expanding the 'failure to prevent' offence to include other economic crime (it currently covers bribery and the facilitation of tax evasion). It concluded that the evidence submitted was inconclusive and that further work was required. The Law Commission was tasked with examining domestic and international models to identify any effective options for reform. On 13 January 2021, a proposed amendment to the Financial Services Bill in 2021, creating a new combined offence of facilitating or failing to prevent certain white-collar offences, was withdrawn before it was debated. On 5 May 2021, the House of Commons library briefing paper on corporate criminal liability was published and, on 9 June 2021, the Law Commission launched its consultation on corporate criminal liability reform. The discussion paper invited responses until 31 August 2021. The Law Commission will analyse the responses and publish an options paper, setting out the options for reform to government.

© Law Business Research 2021

25

United States

Bradley J Bolerjack, Francisca M Mok, Eric H Sussman and Jennifer L Achilles[1]

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The Trump Organization, as the Trump Corporation and other entities are known, is under investigation by local, state and federal authorities regarding a variety of topics. On 1 July 2021, the State of New York indicted two Trump Organization entities and their chief financial officer (CFO), accusing them of involvement in a tax fraud scheme spanning at least 15 years, in which compensation to the CFO and others was significantly underreported. The scheme allegedly included payment of employee rent, tuition and other expenses by the Trump Organization so that taxes for that compensation would not be reported. Conventional wisdom is that other criminal charges could follow for others associated with the Trump Organization. As part of a grand jury investigation, the Manhattan District Attorney prevailed in obtaining former President Trump's personal and corporate tax records after a protracted legal battle that included a US Supreme Court decision.

2 Outline the legal framework for corporate liability in your country.

Under the doctrine of *respondeat superior*, a corporation may be held criminally liable for the illegal acts of its directors, officers, employees and agents. The government must establish that the corporate agent's actions were (1) within the scope of his or her duties and (2) intended, at least in part, to benefit the corporation. The corporation need not have

1 Bradley J Bolerjack and Eric H Sussman are partners in the Chicago office of Reed Smith LLP and Francisca M Mok is the Century City managing partner at Reed Smith LLP. Jennifer L Achilles is a partner with the New York office of Blank Rome LLP.

© Law Business Research 2021

profited from the agent's actions for the corporation to be held liable. Prosecutors in the United States are given broad discretion to determine whether to prosecute for violations of federal criminal law.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are subject to regulation and oversight by federal, state and local authorities depending on their businesses and industry. It is not uncommon for multiple government authorities to conduct investigations at the same time regarding the same set of facts, and agencies do not typically refrain from pursuing cases because other agencies are also involved. The US Department of Justice (DOJ) has policies and protocols relating to corporate prosecutions, as well as a policy to work with other agencies investigating the same conduct to avoid 'piling on' penalties.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

There is no threshold of suspicion that must be met before law enforcement may initiate an investigation. Investigations may even be initiated and conducted to satisfy law enforcement that no misconduct occurred.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Civil subpoenas issued by government agencies can be challenged in court with respect to the lawfulness or scope of a subpoena. However, typically, the relevant government agency has broad authority to obtain information that is relevant to a legitimate subject of investigation.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Both individuals and corporations can benefit from co-operating with law enforcement during an investigation. Individuals may enter into agreements with the government by which they will be granted immunity or be permitted to plead guilty to a lesser charge in exchange for agreeing to provide information or testimony about other defendants. Corporations may receive non-prosecution agreements or deferred prosecution agreements in exchange for co-operating in an investigation.

7 What are the top priorities for your country's law enforcement authorities?

Some top law enforcement priorities affecting corporations include enforcement of the False Claims Act (prohibiting overcharging and related false claims for payment by the government); securities laws regulating publicly traded companies and the stock market;

© Law Business Research 2021

digital assets and cryptocurrency; anti-bribery and anti-corruption laws; cybersecurity; and laws governing consumer online privacy.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

Law enforcement authorities place significant emphasis on whether a compliance programme is adequately resourced and empowered to function effectively. On 1 June 2020, the Criminal Division of the DOJ updated written guidance for prosecutors to reference when evaluating corporate compliance programmes, building on a previous version issued in April 2019. The June 2020 revisions focus on three general questions:

- Is the programme well designed?
- Is the programme being implemented effectively?
- Does the programme work in practice?

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities in your country to cybersecurity-related failings.

The United States does not have an overarching federal cybersecurity law; rather, each state, certain government agencies and banking regulators have created cybersecurity regulations for the corporations under their control.

For example, issuers of US securities are required to comply with the Securities and Exchange Commission's (SEC) regulations, including: (1) Regulation S-P (17 CFR Section 248.30), which requires firms to adopt written policies and procedures to protect customer information against cyberattacks and other forms of unauthorised access; (2) Regulation S-ID (17 CFR Sections 248.201 and 248.202), which outlines a firm's duties regarding the detection, prevention and mitigation of identity theft; and (3) the Securities Exchange Act of 1934 (17 CFR Section 240.17a-4(f)), which requires firms to preserve electronically stored records in a non-rewritable, non-erasable format. Since 2015, the SEC has brought a handful of enforcement actions against public companies for violations of these Regulations.

All 50 US states have state-specific cybersecurity laws, and a few states have laws restricting the use of biometric data such as facial recognition. All states require companies to inform consumers if their personal information has been, or may have been, compromised. In cases of significant breaches, state Attorneys General work together to bring coordinated, multi-state data breach actions. Consumers damaged by data breaches are also permitted to bring private lawsuits and class actions under state law. State banking regulators also have cybersecurity requirements and often coordinate enforcement efforts.

© Law Business Research 2021

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Most cybercrime is prosecuted under the US Computer Fraud and Abuse Act, which criminalises the unauthorised access of a protected computer without proper authorisation. It covers hacking, phishing, infection of IT systems with malware, electronic theft and identity theft or fraud. Additional US statutes that cover cybercrime are 18 USC Section 1028, which criminalises identity theft; 18 USC Section 1029, which criminalises the use of unauthorised access devices to commit fraud; and the Stored Communication Act (18 USC Section 2701), which criminalises electronic theft of stored communications. The US Department of Justice has a Computer Crime and Intellectual Property Section that investigates and prosecutes computer crimes.

The United States and 60 other jurisdictions have signed the Budapest Convention on Cybercrime, which is a binding international treaty that provides a framework for international co-operation on cybercrime and electronic evidence.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In *RJR Nabisco, Inc. v. European Community* (2016), the US Supreme Court set up a two-step framework for addressing the extraterritorial application of federal statutes. First, a court must determine whether the presumption against extraterritoriality has been rebutted through a clear, affirmative indication that the statute applies extraterritorially. If not, the court must determine whether the case involves a domestic application of the statute. If the relevant conduct occurred within the United States, even if some conduct occurred abroad, the case is deemed an acceptable domestic application of the statute. However, if the conduct that is the statute's focus occurred abroad, extraterritorial application is not permitted.

The Foreign Corrupt Practices Act is an example of a statute that indicates that it can be applied against foreign companies or persons who carry out bribery schemes while acting in the United States. Since 2010, the US courts have narrowly construed the extraterritorial reach of a number of other statutes, including the Alien Tort Statute, the Torture Victim Protection Act and the Securities and Exchange Act of 1934.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The combination of data protection regimes, blocking statutes, bank secrecy laws and employment laws outside the United States make cross-border investigations challenging. The US Department of Justice (DOJ) has broad discretion to provide co-operation credit and leniency to corporations that turn over relevant facts in a timely manner. Corporations that have relevant documents outside the United States must weigh the risk of violating foreign laws against the risk that the US government will bring criminal charges against them.

© Law Business Research 2021

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy does not prevent the US government from charging a corporation with a crime even if the corporation has already resolved similar charges with a foreign government. According to the dual-sovereignty doctrine, a crime under the laws of one sovereign is not 'the same offence' for double jeopardy purposes as a crime under the laws of another sovereign.

In May 2018, the DOJ adopted a non-binding policy into the Justice Manual that promotes coordination between US and foreign law enforcement in an effort to limit duplicative penalties on corporate entities for the same conduct. The policy instructs prosecutors that in resolving a case with a company that is being investigated by multiple authorities, the DOJ and others should coordinate with one another to avoid the unnecessary imposition of duplicative penalties against the company.

14 Are 'global' settlements common in your country? What are the practical considerations?

Global resolutions are becoming more common as US law enforcement increases its co-operation with law enforcement in other countries. Global settlements can benefit a corporation by presenting an efficient way to resolve issues with multiple countries at once. However, global settlements do not always result in overall reduced penalties and fines, as combined law enforcement authorities may make higher settlement demands than they would have made individually. Corporations should proceed cautiously when negotiating global settlements and be sure to invoke any applicable policies against 'piling on'.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

A criminal decision against a corporation in another jurisdiction will not end an ongoing investigation in the United States. US law enforcement may attempt to co-operate with foreign authorities to gain additional facts about the corporation that it has been unable to obtain directly. US law enforcement may also consider the penalties and fines imposed by the foreign authority when deciding an appropriate penalty in the United States.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury enforces economic and trade sanctions against targeted foreign countries and individuals,

© Law Business Research 2021

and takes action against those who do business with them. Primary sanctions, which prohibit transactions with sanctioned countries or persons, apply to US persons, US corporations and all persons physically located in the United States, regardless of nationality. Non-US entities can also be liable for primary sanctions for taking actions within the United States, conspiring with US persons to violate sanctions, or using the US financial system. Secondary sanctions may be imposed on non-US persons or entities who engage in transactions deemed to be contrary to US national security and foreign policy interests. Although penalties cannot be imposed for secondary sanctions, they can result in access to the US financial system or markets being restricted. OFAC has brought several high-profile cases against non-US financial institutions in recent years.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

In 2019, OFAC assessed nearly US$1.3 billion in monetary penalties across 30 public enforcement actions. In 2020, enforcement actions decreased steeply to 17 public enforcement actions assessing US$23.5 million. During the first half of 2021, OFAC issued eight enforcement actions resulting in penalties of more than US$133.5 million, which puts OFAC on track to match 2020. The decrease in sanctions activity in 2020 and 2021 likely does not indicate a shift in priorities, but rather disruption arising from the covid-19 pandemic or OFAC resolving lower value cases in its pipeline.

18 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

The US Treasury Department and OFAC co-operate with their counterparts in countries that are allies of the United States.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The United States has not enacted blocking legislation.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

© Law Business Research 2021

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Common ways in which misconduct comes to light include regular audit and compliance activities, whistleblower complaints, government subpoenas, media reports, and business people encountering irregularities in the ordinary course of their jobs.

Under federal securities laws, when auditors become aware that an illegal act may have occurred at a public company, certain affirmative investigation and reporting obligations are triggered. The auditor is obliged to determine whether an illegal act has occurred, report it to management and assure itself that the issuer's audit committee or board of directors has also been informed. Additional reporting obligations are imposed on the auditor if the issue is not remedied, which culminate with auditor withdrawal and affirmative reporting of the issue to the SEC.

INFORMATION GATHERING

22 Does your country have a data protection regime?

The United States does not have a data protection regime.

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

Not applicable.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

Not applicable.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no general restriction on interception of employee communications in the United States so long as employees are using company systems.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Ordinarily, US law enforcement uses subpoenas to obtain documents and other materials from companies. It is unusual for law enforcement to conduct a dawn raid or to execute a search warrant at a company. The use of these tools generally indicates a concern that the

© Law Business Research 2021

company may either conceal or destroy relevant evidence if it was requested by a subpoena rather than physically seized.

A search warrant allows law enforcement to search for materials specifically delineated in the warrant. While a search warrant requires a company to provide access to these materials, it does not require employees of the company to submit to interviews or to answer questions posed by law enforcement. If law enforcement exceeds the limits of a search warrant or conducts improper interviews, the company's primary recourse would be to move to suppress the information in any subsequent legal proceeding.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Law enforcement agencies bear the responsibility for segregating privileged materials or using a special 'taint team' of attorneys unrelated to the investigation to review seized documents for privilege. Ordinarily, companies will not be permitted to withhold privileged documents without the consent of law enforcement. Companies can assist in the privilege review process by identifying in-house and external attorneys to the investigative agents. Companies can also be careful to segregate these materials to protect against inadvertent disclosure.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Under the Fifth Amendment to the US Constitution, an individual cannot be compelled to provide incriminating testimony against himself or herself. Any testimony improperly compelled cannot be used in a legal proceeding against the individual. Companies, however, are not protected by this privilege and cannot withhold testimony that might be incriminating. Generally, there is no right against self-incrimination for producing documents, unless the act of producing the documents would be incriminating.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The United States does not have a comprehensive framework for protecting all whistleblowers in all situations. Instead, many different federal and state laws have been enacted to incentivise whistleblowers and protect them from retaliation. For example, the False Claims Act allows persons and entities with evidence of fraud against federal programmes or contracts to sue the wrongdoer on behalf of the government. A *qui tam* plaintiff can receive between 15 and 30 per cent of the total recovery from the defendant.

Additionally, the whistleblower programme under the Dodd-Frank Act provides monetary incentives for individuals to report possible violations of the federal securities laws to the SEC. Under the programme, eligible whistleblowers are entitled to an award

© Law Business Research 2021

of between 10 and 30 per cent of the monetary sanctions collected. The whistleblower programme also prohibits retaliation by employers against employees who provide the SEC with information.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Aside from any applicable whistleblower protections, employees generally do not have rights under federal or state employment laws during an investigation. This is true whether the employee is an officer, director or rank-and-file employee.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Unless whistleblower protections apply, a company may take any number of disciplinary actions against an employee who has engaged in misconduct, including suspension or dismissal. US public companies have a duty to their shareholders to take action and not turn a blind eye to misconduct.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Most employees in the United States are subject to at-will employment, meaning that, unless other protections apply, their contracts may be terminated at any time. Employees whose conduct is within the scope of an investigation are expected to participate in investigations, and may be dismissed if they refuse to co-operate.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common to have a working investigative plan to manage investigative activities. Such a document may address:

- document preservation and gathering;
- witnesses;
- legal issues and analysis;
- factual analysis;
- key questions to be answered; and
- reporting obligations.

© Law Business Research 2021

However, because investigations are often fluid, the expectation is that the document will be updated and revised frequently, to account for new or different tasks based on information learned in the course of the investigation.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

A company should conduct an internal investigation and remediate the issue. Most government agencies give corporations credit for investigating and self-reporting issues. The decision to self-report is fact dependent and involves weighing many factors.

Under the Securities and Exchange Commission's (SEC) regulations, an in-house lawyer at a public company is required to report 'evidence of a material violation' to the issuer's chief legal officer and chief executive officer, and in some cases to the appropriate committee of the issuer's board of directors consisting solely of independent directors, or to the whole board of directors. In the context of an investigation initiated by a public company's external auditors, the company may have an obligation to report to the SEC if the auditors conclude that the company has not properly remediated certain illegal activities.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

The company should prepare a legal hold notice and distribute it to relevant individuals and the company's IT department. Affirmative steps should be taken to prevent destruction of responsive materials – including discontinuing any automatic deletion of such data pursuant to data retention policies.

If the company is being investigated for potential wrongdoing, it is important that external counsel or individuals with indicia of independence and trustworthiness are responsible for preserving and collecting documents. If there is any uncertainty regarding what search terms should be used to identify responsive documents, attorneys for the corporation typically discuss search terms with the government.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

As a general matter, there is no requirement to disclose the existence of an internal investigation or the fact that the company has been contacted by law enforcement. Public companies are forbidden from making affirmative statements that are false or misleading. Thus, companies should be careful not to make statements that are untrue or misleading because of undisclosed facts about an internal investigation or law enforcement contact. There is a duty to disclose to the extent that disclosure is necessary to ensure affirmative statements are not misleading.

© Law Business Research 2021

37 How are internal investigations viewed by local enforcement bodies in your country?

Government authorities place value on independent and thorough internal investigations. For example, the US Department of Justice in its Justice Manual has stated that to 'earn maximum cooperation credit, a corporation must do a timely self-analysis and be proactive in voluntarily disclosing wrongdoing and identifying all individuals substantially involved . . . or responsible' (Section 4-3.100(3)). The SEC describes self-reporting as one of the key factors for evaluating a company's co-operation, 'including conducting a thorough review of the nature, extent, origins and consequences of the misconduct, and promptly, completely and effectively disclosing the misconduct to the public, to regulatory agencies, and to self-regulatory organizations' (SEC Enforcement Manual, Framework for Evaluating Co-operation by Companies, 6.1.2). Neither agency sets forth exacting requirements for the conduct or format of the internal investigations; what is appropriate is fact-dependent.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Generally, the attorney–client privilege and the attorney work-product doctrine may be claimed over most aspects of an internal investigation so long as the fact-finding and analysis is being done by or at the direction of attorneys for the purpose of providing legal advice to the client. This privilege would cover attorney notes, interview memoranda, legal analysis and recommendations provided by counsel to the client. Companies should ensure that privileged materials are not shared with third parties and are clearly labelled as being 'attorney–client privileged'.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Communications by corporate employees made for the purpose of assisting counsel in providing legal advice to the corporation are generally covered by attorney–client privilege. The corporation holds the privilege and it may only be waived by the corporate entity or an authorised executive (for example, the general counsel).

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege applies equally to in-house and external counsel so long as both are providing legal advice. In certain instances, in-house counsel will be called on to provide 'business' advice, which is not protected even if it is provided by an attorney.

© Law Business Research 2021

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The attorney–client privilege applies equally to US and foreign lawyers.

42 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

While the waiver of the attorney–client privilege is regarded as a co-operative step by US law enforcement, US Department of Justice policy prohibits law enforcement from requesting or requiring privilege waivers to receive credit for co-operation. Other federal agencies may request but do not typically require privilege waivers to obtain co-operation credit.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Most courts will not enforce 'selective waivers' to government entities. Companies sometimes provide factual information to the government (rather than any legal analysis or memos) to avoid an argument by a third party that privilege has been waived.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If the disclosure of attorney–client information was compelled in a foreign country (or the privilege was not recognised), this would generally not result in a waiver of the attorney–client privilege in the United States. However, any voluntary disclosure will usually result in a waiver.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in the United States. It is an extension of the attorney–client privilege to communications between two or more parties that have a common legal interest. The party asserting the privilege must demonstrate that (1) the communications were made in furtherance of a joint defence effort, (2) the statements were designed to further that effort and (3) the privilege was not waived.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

So long as a third party is working for a client at the direction of an attorney, and for the purpose of assisting the lawyer to provide legal advice to the client, this assistance will remain privileged.

© Law Business Research 2021

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, witness interviews are a critical part of internal investigations in the United States.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

Yes, companies regularly assert privilege over witness interviews and reports in the United States, provided that the interviews and reports were generated to provide legal advice.

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Upjohn warnings are required when conducting witness interviews of employees and are typically provided to both current and former employees.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Witness interviews are typically conducted by external counsel, sometimes in the presence of in-house counsel or subject-matter experts assisting counsel (or both). Documents are usually shown to the witness during interviews. Witnesses can retain their own legal representation if they so choose, but there is no requirement to do so.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no overarching duty or legal obligation to self-report corporate misconduct, but there are certain specific situations in which it is mandatory, including highly regulated industries such as insurance, banking and healthcare.

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The US Department of Justice and several other federal agencies have issued policies providing for leniency and reduced penalties for companies that self-report. It is generally understood that co-operating with a government investigation will not result in as favourable an outcome for a corporation as the combination of self-reporting and co-operating. In some cases, self-reporting corporate misconduct and co-operating with an investigation can lead to a decision not to prosecute.

© Law Business Research 2021

Despite the strong incentive to self-report, it is not always the best course of action. Several factors must be considered, such as the severity and pervasiveness of the misconduct, whether corporate officers or board members were involved, whether the misconduct continued for a long period, and whether the investing public or consumers were harmed by the misconduct.

53 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no formal process for self-reporting. Typically, external counsel will contact prosecutors or regulators and seek a meeting to explain how the misconduct was discovered, how the misconduct occurred, and what the corporation is doing to investigate and make sure the misconduct is not repeated. One of the factors the government considers is whether the company reported within a reasonable time after learning of the misconduct. Accordingly, a complete internal investigation is not required prior to self-reporting, although the company will want to understand enough facts to determine whether self-reporting is advisable.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The first step following receipt of a subpoena would ordinarily be for external counsel to make a call to the government attorney. The purpose of the call would be to understand the nature and scope of the government's investigation, as well as whether the company is a target of the investigation or simply a witness. Most law enforcement agencies will enter into a dialogue with a company's external attorney prior to charges being brought. Most prosecutors' offices will also allow companies' attorneys to meet with senior supervisors in the relevant prosecutor's office to present their position as to why charges should not be brought.

55 Are ongoing authority investigations subject to challenge before the courts?

Investigations are considered to be firmly within the discretion of the executive branch of government. Unless there is evidence that government prosecutors are abusing their investigative authority and violating legally protected rights, it is highly unusual for courts to interfere with an ongoing investigation.

© Law Business Research 2021

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

When a company receives multiple subpoenas regarding the same facts, the company should analyse whether this is part of a coordinated effort or whether these are entirely separate investigations. If they are coordinated investigations, it can be advantageous to ensure consistent disclosure between all jurisdictions. If they are separate investigations, it may not be advantageous to alert US authorities that foreign authorities are investigating the same issues.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Prosecutors typically expect a company to search for and produce responsive documents in its possession, custody or control even if those documents are located outside the United States. Documents held by a company's foreign affiliates are generally considered to be in the company's control. If the subpoenaed documents implicate the laws of another jurisdiction, such as data privacy laws, the company should consider whether there is a way to comply with the law while also complying with the subpoena (such as by requesting the consent of employees whose data will be turned over). If responding to a subpoena would expose a company and its employees to criminal liability in another country, the company may decide to seek a protective order from a US court.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

It is common for US law enforcement to share investigative materials with authorities outside the United States, particularly when the information sharing is mutual. Sometimes co-operation occurs through formal mutual legal assistance treaties or memoranda of understanding.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Unless law enforcement agrees to be bound by a non-disclosure agreement, the government can share materials received during an investigation with other agencies or overseas investigators. The government does not typically share information with non-government third parties or allow the material to be subject to public disclosure during the course of an investigation. There are strict secrecy laws for information obtained in the United States

© Law Business Research 2021

via a grand jury subpoena. This information cannot be shared without a court order, or else under very narrow legal exceptions.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A company should not voluntarily produce documents to US law enforcement if doing so would violate the laws of another country. If the company is compelled to produce documents by subpoena, the least risky solution is to obtain consent from the foreign country or ask law enforcement to obtain the documents through a mutual legal assistance treaty. If those options fail, the company could seek a protective order in court, seeking to be relieved of its obligation to produce such documents. If the court denies the company's motion for a protective order, the company will have to decide whether it is more risky to continue to resist the subpoena or to comply and violate foreign law.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Not applicable.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In some cases, there are no additional risks in producing documents voluntarily than there are pursuant to a subpoena. In other cases, however, such as when the government requests otherwise confidential information about customers or third parties, it is less risky to produce documents pursuant to a subpoena. Voluntary production may subject a company to potential liability from third parties for providing confidential information to law enforcement that was not compelled.

Documents produced to the government during the course of an investigation are exempt from public disclosure under the Freedom of Information Act during the pendency of the investigation. Information compelled by a grand jury subpoena is ordinarily protected by strict secrecy and would not be discoverable by third parties, whereas similar information that was voluntarily provided would be discoverable.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

If a company is convicted of a crime, it can be sentenced to fines, restitution, disgorgement, forfeiture of property derived from criminal activity, and suspension or debarment. Corporate monitors are also sometimes appointed to oversee a company's ongoing

© Law Business Research 2021

activities. Individuals are subject to similar criminal penalties, in addition to possible imprisonment and other potential collateral consequences.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Depending on the context of an investigation, suspension or debarment is a significant risk in heavily regulated industries, such as healthcare and securities. When negotiating with regulators, counsel may be able to negotiate terms that would avoid or minimise the risk of these possibilities and the attendant impact on future business operations. Extraterritorial settlements are not typical because such arrangements tend not to resolve violations of US law.

65 What do the authorities in your country take into account when fixing penalties?

In the event of federal criminal conviction, sentencing courts consider factors set forth in the US Sentencing Guidelines as well as criminal statutes and policy guidelines. In general, the broad factors to be considered at sentencing are set forth at 18 USC Section 3553(a) and include:

- the nature and circumstances of the offence and the history and characteristics of the defendant;
- the need for the sentence imposed to reflect the seriousness of the offence, promote respect for the law and provide just punishment for the offence;
- to afford an adequate deterrent to criminal conduct;
- to protect the public from the defendant committing further crimes;
- to provide the defendant with the necessary educational or vocational training, medical care or other correctional treatment in the most effective manner;
- the kinds of sentences available;
- the kinds of sentences and the sentencing range established for the applicable category of offence committed by the applicable category of defendant as set forth in the US Sentencing Guidelines or applicable policies; and
- the need to provide restitution to any victims of an offence.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Both are available in the United States.

Under the terms of a non-prosecution agreement (NPA), the government agrees not to file a criminal charge for the specified acts under investigation. In exchange, the putative corporate or individual defendant enters into certain agreements with the government, which may include financial terms, imposition of a corporate monitor or other remedial actions. The advantage of such an agreement from the defendant's perspective is that no

© Law Business Research 2021

criminal charge is filed and no conviction for any offence occurs (provided that the terms of the NPA are satisfied).

Under the terms of a deferred prosecution agreement (DPA), the government agrees to hold in abeyance a criminal charge that has already been filed in exchange for the defendant's agreement to undertake certain actions. This can include financial requirements, monitoring requirements and other conditions, depending on the nature of the case. The advantage of a DPA is that, provided the terms of the agreement are satisfied for the designated period, the government agrees to dismiss the pending criminal case and no criminal conviction results.

The disadvantage of NPAs and DPAs is that the facts of the case are never tested by the adversarial system in court. Therefore, the government can make demands and allegations without ever having to prove, or even provide supporting evidence to establish, that a crime actually may have occurred.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no restriction on reporting the existence or terms of a DPA or NPA.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before entering into any settlement or plea bargain, companies must fully assess the risks and costs associated with trial, which involves a critical and detailed analysis of the underlying facts. If a settlement or plea bargain is the appropriate mechanism to resolve the case, companies must consider the effects on business operations and the possible ramifications for suspension, debarment, exclusion, negative publicity, effect on the company's market valuation, or other collateral consequences that may result. Companies should be aware that a resolution with US law enforcement could prompt investigations in other jurisdictions as well as possible private civil litigation, whether in the United States or abroad.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Corporate compliance monitors are used regularly in the context of negotiated resolutions with the US Department of Justice.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private civil rights of action are sometimes allowed by statute. For example, securities fraud may give rise to private civil claims. Private litigants generally do not have access to the government's files, particularly any materials in possession of the government that

© Law Business Research 2021

were obtained via grand jury subpoena, since such materials are protected by Rule 6(e) of the Federal Rules of Criminal Procedure.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

At the investigatory stage, all matters being investigated by a grand jury are protected from public disclosure by the government. Although a company is free to disclose the existence of an investigation if it so chooses, this usually does not happen unless the company decides that the existence of an investigation should be made known to shareholders or other parties of interest.

Once a case is before a court, the court record and pleadings in the case are generally available to the public, unless the case is filed under seal. The general view is that court cases should be transparent unless there is a special reason for confidentiality being required.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Public relations firms are commonly used to assist with corporate messaging strategy. However, careful coordination between public relations firms and counsel is of paramount importance. Although a statement may be good for the company from a public relations perspective, that same statement may be harmful to the company from a criminal law perspective, and such statements may be admissible in the event of a trial or other proceeding on the merits.

73 How is publicity managed when there are ongoing related proceedings?

All publicity should be managed through the company's counsel. Counsel should coordinate and manage media issues in connection with public relations professionals.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under securities laws governing US issuers, disclosure would be required if a corporation's prior disclosures about a matter would be misleading without the updated information. Disclosure may also be required if the nature of a settlement triggers affirmative reporting obligations, for instance under the Securities and Exchange Commission's Regulation S-K.

© Law Business Research 2021

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE (ESG)

75 Does your country regulate ESG matters?

Although the Biden Administration is widely expected to encourage the regulation of US businesses regarding ESG issues, the United States does not currently regulate these matters beyond imposing a general duty on US public companies to disclose ESG matters that are material to their businesses.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address ESG matters?

In 2021, the Securities and Exchange Commission (SEC) has taken several actions with respect to ESG, including discussing climate-related and ESG-related issues in its 2021 Examination Priorities Report, requesting public comment on issues relating to ESG, and forming an ESG enforcement task force. Additionally, the Biden Administration issued an Executive Order in May 2021 declaring that it is the policy of the United States to 'advance consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk' and 'to mitigate that risk and its drivers, while accounting for and addressing disparate impacts on disadvantaged communities and communities of color'.

On 16 June 2021, the US House of Representatives passed legislation, by a very slim margin, that would impose new ESG due diligence and disclosure requirements on US public companies. If the US Senate passes the bill and the bill is signed into law, it would require public companies to disclose ESG metrics as well as the link between those metrics and the company's long-term business strategy. The bill also calls for the SEC to determine which ESG metrics public companies should be required to disclose, noting that the SEC may incorporate disclosure standards implemented by other jurisdictions.

77 Has there been an increase in ESG-related litigation, investigations or enforcement activity in recent years in your country?

In March 2021, the SEC announced the creation of a new climate and ESG task force in the Division of Enforcement. According to the press release announcement, the initial focus of the task force would be to identify any material gaps or misstatements in public company disclosure of climate risks under existing rules. At the time of writing, there were no enforcement actions brought by the new ESG task force; however, the SEC indicated that the public could expect to see more cases like the one it brought in September 2020 against an automotive company. In that case, the SEC claimed that the company made misleading disclosures about an internal audit of its emissions control systems and failed to include a comprehensive review of its compliance with US emissions regulations. The company settled the case for US$9.5 million without admitting or denying the allegations.

© Law Business Research 2021

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The Anti-Money Laundering Act of 2020 (AMLA) became US federal law on 1 January 2021. AMLA provides for expanded whistleblower protections, enhanced subpoena power over foreign bank accounts, larger penalties for money laundering violations, and the establishment of a beneficial ownership registration database that will be implemented by the US Financial Crimes Enforcement Network (FinCEN). AMLA also codifies FinCEN's earlier guidance that companies that exchange or transmit virtual currencies qualify as money transmitters and must comply with the Bank Secrecy Act.

The Corporate Transparency Act, which is part of AMLA, will require new and existing corporations, limited liability companies and other similar entities to report personal identifying information to FinCEN for their natural-person beneficial owners and for the applicants who establish or register the entities. The Act requires FinCEN to issue proposed rules implementing this provision by January 2022, and to consult with the US Department of Justice and other relevant agencies on the appropriate scope of the rules.

© Law Business Research 2021

Appendix 1

About the Authors of Volume II

Jennifer L Achilles
Blank Rome LLP

Jennifer Achilles is a partner in Blank Rome's white-collar defence and investigations group based in New York. Her practice focuses on white-collar criminal defence, securities litigation and internal investigations. Jennifer is regularly ranked as a super lawyer and is an active supporter of diversity initiatives. She defends public and private companies, their officers and directors, in insider trading, market manipulation, fraud, antitrust and Foreign Corrupt Practices Act investigations by the SEC, CFTC, FINRA, DOJ and New York District Attorney's and Attorney General's offices. Jennifer also leads internal investigations in advance of and in connection with government investigations, and counsels clients on co-operation and self-disclosure strategies.

Ama A Adams
Ropes & Gray LLP

Ama A Adams is a litigation and government enforcement partner at Ropes & Gray in Washington, DC. Her practice focuses on international transactions and the US government's regulation of trade and investment. This includes, most notably, export controls, economic sanctions, anti-corruption, foreign direct investment and customs laws and regulations. In addition to advising clients on the application of international trade regulations to their business operations, Ms Adams also assists clients in developing compliance programmes, handling pre- and post-acquisition due diligence, conducting internal investigations relating to potential violations of trade laws and representing clients before the US government agencies in connection with enforcement matters and government inquiries. She advises companies in a range of industries, including the oil and gas, aviation, pharmaceutical, manufacturing, technology, chemical and financial sectors.

© Law Business Research 2021

Pamela Alarcón Arias

Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pamela Alarcón Arias is a partner at PPU and an expert in criminal law and compliance. She is also an attorney and consultant in criminal law, corporate criminal law, corruption, crime prevention and compliance, as well as risk analysis in corporate business and criminal litigation. She has an outstanding reputation for managing crises arising from criminal activities within companies, by advising legal representatives, chief executive officers, managers and administrators. She is also a criminal consultant and provides risk analysis in real estate, financial, matters relating to mergers and acquisitions and infrastructure, among other things. She has extensive experience in corporate criminal law, as well as corruption and criminal compliance issues.

Pamela has degrees in law and political science from Los Andes University, a master's degree in advanced studies of human rights from the Carlos III University in Madrid and a specialist degree in corporate law from the Pontifical Xavierian University in Bogotá. She is a former adviser to the Office of the Deputy Attorney General and a professor of corporate criminal law and compliance at various universities in Bogotá.

Jaime Alonso Gallo

Uría Menéndez Abogados, SLP

Jaime Alonso Gallo joined Uría Menéndez as a partner in 2013. He previously worked for Estudio Jurídico Rodriguez Mourullo, one of Spain's most renowned criminal law firms.

Based in the Madrid office, Jaime specialises in white-collar crime and, in particular, crimes relating to listed companies and financial markets, tax fraud, urban planning and environmental crimes. He also specialises in criminal compliance (compliance programmes, anti-bribery compliance, internal investigations, etc.).

Ilias Anagnostopoulos

Anagnostopoulos

Ilias Anagnostopoulos has appeared as lead counsel in most of the significant corporate and criminal cases in Greece during the past 30 years and is a professor of criminal law and criminal procedure at the School of Law, National University of Athens. He has extensive experience in most types of business crime, financial fraud, European criminal law, tax and customs fraud, healthcare and procurement fraud, medical malpractice, product criminal liability, environmental liability, compliance, money laundering, corruption practices, anticompetitive practices and cartel offences, anti-terrorism, extradition and mutual assistance. His many publications in Greek, English and German deal with matters of Greek, European and international criminal law, business and financial crimes, reform of criminal procedure and human rights.

He is chair of the Hellenic Criminal Bar Association (since 2013) and has chaired the Criminal Law Committee of the Council of the Bars and Law Societies of Europe (2007–2013). Memberships include the Criminal Law Experts Commission (Ministry of Justice), the High Legal Council with the Bank of Greece and FraudNet of the International Chamber of Commerce.

© Law Business Research 2021

Caitlin Anyon-Peters
Meredith Connell

Caitlin Anyon-Peters is a solicitor in the commercial litigation team where she provides advice and advocacy services for a broad range of corporate clients and government bodies. She also acts for the Crown in criminal proceedings.

Before joining Meredith Connell, she spent two years as a judge's clerk at the Court of Appeal where she worked on both civil and criminal matters.

Caitlin has an LLB (Hons) and a BA from the University of Auckland.

Claudio Bazzani
Homburger

Claudio Bazzani is a partner and co-head of Homburger's white-collar and investigations team and litigation and arbitration practice. He specialises in internal and regulatory investigations and advises corporate clients in compliance matters. He represents clients in investigations by Swiss and foreign authorities as well as in domestic and international litigation and arbitration proceedings.

Claudio Bazzani has more than 10 years of experience in conducting large-scale internal and regulatory investigations. He regularly advises and represents clients in financial market compliance issues and has profound knowledge of the legal and practical challenges Swiss companies face in cross-border matters.

Eike Bicker
Gleiss Lutz

Dr Eike Bicker is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Eike advises national and international clients on corporate law and compliance. He is a specialist in strategic compliance advisory and (cross-border) compliance investigations. He has particular expertise in corporate governance issues, board matters and company group law issues.

Eike studied at the universities of Saarbrücken, Freiburg and Cambridge (LLM 2005). He has been with Gleiss Lutz since 2015. Eike was previously a partner at a prestigious compliance boutique firm in Frankfurt. Eike speaks German and English.

Bradley J Bolerjack
Reed Smith LLP

Bradley J Bolerjack is a partner in Reed Smith's regulatory and investigations group in Chicago, where he focuses on complex criminal law matters, including sensitive internal investigations, grand jury investigations, compliance counselling and trial practice. Recent engagements have included investigations or indictments (or both) relating to the Foreign Corrupt Practices Act, commercial bribery, antitrust cartels, healthcare fraud, tax evasion, white-collar fraud and government contracting fraud. Brad has been notably successful in avoiding indictment of numerous high-profile clients even after they have received target status. In cases that are indicted, Brad has obtained outstanding results for many clients,

© Law Business Research 2021

whether through trial or negotiated resolutions. His clients include consumer product, medical device, pharmaceutical, manufacturing and other domestic and international companies, as well as individuals.

Michael Bowes QC
Outer Temple Chambers

Michael Bowes QC specialises in business crime, corruption, civil fraud, financial services and economic sanctions. He acts for corporate clients and senior managers in global investigations and for the SFO, FCA, CMA and Lloyd's of London. He advises companies in respect of US and EU sanctions. He acts for overseas regulators and is instructed in overseas cases as an expert in English law. He is regarded as an expert in civil and criminal 'cross-over' work and is described as 'one of the few specialist criminal practitioners in this area' (*The Legal 500* 2015) and as '[v]ery clever and has wide expertise, so is comfortable with criminal and civil work' (Financial Crime: Corporates, *Chambers* 2017). He is listed as a leading silk in the fields of financial services, financial crime (corporates) and financial crime (London) in *Chambers* 2017, and for banking and finance, business and regulatory crime, and fraud in *The Legal 500*. He is listed in *Who's Who Legal* 2016 as an expert in business crime defence. He is a joint head of Outer Temple Chambers. He sits as a Deputy High Court Judge (Queen's Bench Division) and as a Recorder of the Crown Court. He is a Bencher of the Honourable Society of the Middle Temple. He is a trustee of Transparency International UK and a co-chair of the UK Chapter of the International Section of the New York State Bar Association.

Santiago Breton
Claro y Cia

Santiago Breton is an associate at Claro y Cia, where he focuses on litigation and criminal law. He joined the firm in 2021. He is a professor's assistant in criminal law at the Pontifical Catholic University of Chile. Previously, he was also a professor's assistant in history of law at the same university. Santiago Breton gained his JD from the Pontifical Catholic University of Chile in 2020.

John D Buretta
Cravath, Swaine & Moore LLP

John D Buretta is a partner in Cravath's litigation department and a former senior official at the US Department of Justice (DOJ). He has represented global companies, boards of directors, audit committees, senior management and general counsels of public and private companies, law firms, and former US and foreign government officials with respect to internal investigations, criminal defence, regulatory compliance and related civil litigation matters. He has handled matters involving the US Foreign Corrupt Practices Act (FCPA), antitrust laws, securities fraud and disclosure regulations, money laundering and anti-money laundering controls, trade sanctions, export controls, cyber intrusion and tax compliance, and has appeared for clients before numerous US enforcement agencies.

© Law Business Research 2021

Mr Buretta served for 11 years in the DOJ, including supervising the Criminal Division, where he oversaw nearly 600 prosecutors in international investigative matters involving corporate fraud, the FCPA, insider trading, healthcare fraud, money laundering, the Bank Secrecy Act, trade sanctions, asset forfeiture, cybercrime, intellectual property theft and public corruption. He currently serves as an independent monitor in separate appointments by the DOJ and the US Department of Transportation.

María González Calvet

Ropes & Gray LLP

María González Calvet serves as co-chair of the firm's award-winning global anti-corruption and international risk practice and Latin America initiative. She was formerly a trial attorney in the US Department of Justice's Criminal Division, Fraud Section, and was a member of the Foreign Corrupt Practices Act Unit. She was also an in-house executive counsel of a Fortune 500 company.

With a practice that spans two decades, María has conducted internal and government investigations in more than 40 countries around the globe arising from whistleblower complaints, escalations from audits and other front-end monitoring, and benchmarking. Drawing on her former work in government and the corporate sector to help multinational clients across industries, including aerospace, life sciences, energy and private equity, María also works with clients to identify and mitigate corruption risks and to implement effective compliance programmes.

María is widely recognised as a thought leader in anti-corruption, particularly on anti-corruption risks and enforcement trends in Latin America, and is frequently quoted in the press for her expert commentary. María also regularly presents at major industry-leading conferences across the globe and hosts webinars, roundtables and podcasts on emerging issues in anti-corruption and compliance.

María is a fluent, native Spanish speaker and an advanced Portuguese speaker.

Connor Cassidy

Matheson

Connor Cassidy is a senior associate in the regulatory and investigations team within the commercial litigation and dispute resolution practice. He has more than eight years' experience in advising a wide range of clients in all aspects of dispute resolution. In particular, he has significant experience in corporate crime matters and investigations and regularly advises both domestic and international clients in respect of regulatory investigations and enforcement actions, bribery, corruption, fraud and money laundering offences along with related compliance issues. He also represents clients in large-scale civil litigation, including in relation to civil fraud, product liability, shareholder disputes, commercial and financial services disputes, professional negligence and debt recovery.

Connor joined Matheson in 2016 having previously practised as a barrister in Northern Ireland. Connor has been involved in a number of the most significant regulatory enforcement actions by the Central Bank of Ireland of recent times. He has advised clients in relation to regulatory inspections, investigations and administrative sanctions

© Law Business Research 2021

arising from governance, anti-money laundering, financial crime controls and disclosure requirements. Connor was recognised as a key lawyer in white-collar crime in *The Legal 500* 2021 rankings.

Marcin Ciemiński
Clifford Chance

Marcin Ciemiński specialises in disputes before state courts and arbitral tribunals, including commercial disputes, public procurement, intellectual property, damages and healthcare cases.

Marcin is also responsible for handling matters concerning white-collar crime, criminal investigations, compliance and crisis management. He advises healthcare and life sciences clients on regulatory issues. As an assistant professor, he lectures in commercial law at the Warsaw University.

Tracey Cui
Herbert Smith Freehills

Tracey Cui advises multinational and regional corporates operating in China on investigations and compliance matters, commercial dispute resolution and international arbitration. She has a particular focus on investigations and compliance issues that arise under China's criminal law and anti-unfair competition law. Tracey has spent time on secondment at multinational corporates advising on anti-corruption investigations and compliance matters.

Tracey passed the PRC National Bar Exam in 2009. She is fluent in Mandarin and English, and is based in Shanghai.

Robert Dalling
Jenner & Block London LLP

Robert Dalling is a partner in Jenner & Block's investigations, compliance and defence practice. Formerly a trial advocate with 10 years' courtroom experience, he has represented global financial institutions, multinational corporates and individuals in high-profile and high-value internal and external investigations involving a wide range of financial crime and other regulatory issues.

Rob has advised some of the world's largest financial institutions on financial sanctions, often in connection with complex and sophisticated financial products and transactions. He has experience in applying for licences from sanctions authorities in the United Kingdom. He advises companies on the development of internal policies (including on anti-bribery, anti-fraud, anti-money laundering and terrorist financing, conflicts of interest, gifts and hospitality, and supply chain and modern slavery issues) and associated procedures, controls and training. He has assisted several clients with complex anti-money laundering issues and has dealt with the National Crime Agency on a large number of consent applications.

© Law Business Research 2021

Prior to moving into private practice, Rob spent several years practising as a barrister in white-collar criminal litigation. Market commentators for *Chambers and Partners* 2020 describe him as an 'excellent' lawyer who is 'incredibly clever and very tactical'.

Eleanor Davison

Fountain Court Chambers

Eleanor Davison is a barrister at Fountain Court Chambers specialising in cross-border white-collar crime, fraud, corruption and contentious regulatory cases. Consistently recognised as expert in the fields of financial crime, financial crime (corporates), financial services and money laundering, by *The Legal 500* and *Chambers and Partners*, she has recently been described as having 'a phenomenal brain and in-depth knowledge of her area of expertise. She is quick-witted, alert to opposing arguments and a delight to work with – a real star to watch' (*Chambers and Partners UK* 2019, Financial Crime). The directories also describe her as '[v]ery good and particularly experienced in complex investigations involving financial institutions'. Eleanor was listed in *Who's Who Legal* as a Future Leader in investigations in 2018.

Stéphane de Navacelle

Navacelle

Stéphane de Navacelle has worked in the field of white-collar crime and corporate crime in New York, London and Paris (at Engel & McCarney and Debevoise & Plimpton LLP).

With extensive experience in French and US white-collar crime, he has participated in landmark cases involving FCPA and embargo restrictions (OFAC), market abuse and insider trading, fraud (Forex), benchmark manipulation (LIBOR/Euribor), investigations by development banks and criminal and internal investigations in Europe, the Americas and Africa. He is a member of the French Independent Committee on sexual abuse within the Church.

Stéphane was appointed independent compliance monitor – pursuant to a World Bank negotiated resolution agreement – by European infrastructure groups with global operations. He is member of the Paris Bar Council and an ethics investigator.

Monika Diehl

Clifford Chance

Monika Diehl focuses on commercial and investment arbitration, as well as internal investigations and compliance.

She has many years' experience in representing clients in complex litigation and international arbitration disputes spanning a variety of sectors, including renewables, oil and gas, construction and finance. She acts for clients in investment treaty arbitrations.

Monika also has extensive experience in conducting cross-border internal investigations related to white-collar crime and regulatory issues. She regularly advises, conducts training and authors publications on compliance and anti-corruption.

© Law Business Research 2021

Enrico Di Fiorino
Fornari e Associati

Enrico Di Fiorino is a partner at Fornari e Associati. He specialises in white-collar crime (serious fraud, tax evasion, bankruptcy, corporate crimes, market abuse) and is a criminal defence counsel. He also has particular expertise in environmental offences, anti-money laundering and medical malpractice.

Enrico advises companies and individuals in criminal inquiries and represents them in criminal proceedings. He has dealt with cases of criminal, internal and regulatory investigations.

He represents clients in extradition proceedings and cases relating to European arrest warrants and has gained substantial experience with international clients. He writes articles on criminal matters and is regularly a speaker at conferences for executives, lawyers, accountants and students.

He is an academic fellow and lecturer on the Master's in Corporate Tax Law programme at Bocconi University. He is also a lecturer on the Master's in Made in Italy, Fashion and Luxury Management programme at LUM University; the Master's in Decontamination of Polluted Sites at La Sapienza University of Rome; the Master's in Economic, Corporate and Financial Crimes programme at the 24ORE Business School; and the Master's in Corporate Law programme at the 24ORE Business School.

He is a member of the European Criminal Bar Association, European Fraud and Compliance Lawyers, Extradition Lawyers' Association, International Bar Association, Victims of Crime Association of Lawyers, Milan Criminal Bar Association, AODV231 and Transparency International Italia.

Felipe Noronha Ferenzini
Trench Rossi Watanabe

Felipe Noronha Ferenzini joined the firm in 2009. He has more than a decade of practice in the field of compliance, regulatory and administrative law, assisting public and private clients in national and multi-jurisdictional operations and investigations. Felipe has vast experience in the compliance area, structuring and leading complex internal investigations, implementation of compliance, risk and governance programmes (risk assessment, internal policies, remediation mechanisms and training). He also has extensive experience in advising foreign and Brazilian companies regarding compliance laws (Brazilian anti-corruption laws, the US Foreign Corrupt Practices Act, money laundering and regulatory compliance, pharma, oil and gas, and banking, among other things) and dealing with relevant stakeholders (authorities, regulators, internal and external auditors, boards of directors, regulatory agencies and independent oversight committees).

Felipe Noronha Ferenzini is a former lecturer of the postgraduate course on compliance at IBMEC-RJ and is an alumnus of the International Anti-corruption Academy (scholarship for the Summer Academy). He is certified by the Association of Certified Fraud Examiners and the Association of Certified Anti-Money Laundering Specialists. He is recognised by LACCA as one of the leading lawyers in compliance in Brazil.

© Law Business Research 2021

Reto Ferrari-Visca
Homburger

Reto Ferrari-Visca is an associate of Homburger's white-collar and investigations team and litigation and arbitration practice. He specialises in domestic and international litigation and administrative proceedings. He has broad experience in internal and regulatory investigations and advises corporate clients in regulatory and compliance matters. His practice also focuses on privacy and data protection law and he regularly advises clients on cross-border privacy and data protection issues.

William Fotherby
Meredith Connell

William Fotherby's practice consists of civil litigation, criminal prosecution and advice, and internal investigation work.

William first worked for Meredith Connell between 2010 and 2014, when he successfully argued cases for public and private clients at all levels of the New Zealand judiciary including the Supreme Court. He graduated with first-class honours from the University of Cambridge, England, in 2015.

Between 2015 and 2019, he worked as an attorney in the London office of Dechert LLP, an American law firm, in one of the best white-collar-crime practices in the world. He was called to the English Bar (Middle Temple) in 2017. William returned to Meredith Connell in 2019.

Héctor Gadea
Rebaza, Alcázar & De Las Casas

Héctor Gadea is a graduate lawyer from the Pontifical Catholic University of Peru. In 2014, he was awarded an LLM by Columbia University, New York. In addition, he holds a master's degree from the universities of Barcelona and Pompeu Fabra (Spain). Héctor is certified by the Society of Corporate Compliance and Ethics as a compliance and ethics professional.

Héctor is a partner at the firm, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former criminal law lecturer at the Pontifical Catholic University and the Peruvian Judiciary Academy. He has participated as a speaker at a number of international conferences and events.

João Augusto Gameiro
Trench Rossi Watanabe

João Augusto Gameiro became a partner at the firm in 2018. He has more than a decade of experience in criminal law and compliance. As a criminal lawyer, he has represented several multinational companies and their shareholders and directors in police inquiries, criminal proceedings, administrative proceedings and parliamentary committees of inquiry in cases of tax evasion, environmental crimes, consumer crimes, antitrust, corruption, trademark and patent infringement, unfair competition, money laundering and currency evasion. He has also provided legal advice to foreign companies regarding Brazilian criminal

© Law Business Research 2021

law, participated in due diligence projects focused on criminal liability and exposure to anti-corruption and anti-money laundering legislation, and has conducted internal investigations into corporate fraud and competitive violations.

Mr Gameiro holds a law degree (2003) and a master's degree in criminal law (2007) from the University of São Paulo and a postgraduate degree in economic criminal law (2014) from the University of Coimbra. He attended the intensive corporate compliance and ethics course at New York University in 2015.

Laura Gillespie
Pinsent Masons LLP

Laura Gillespie is a partner at Pinsent Masons, qualified in Northern Ireland. Laura has over 20 years' experience in the jurisdiction. She has particular experience in internal investigations and has been involved in a range of international investigations, specialising in data protection. Laura also handles civil fraud, complementing her investigation experience. She also regularly helps clients with board-level training and policy implementation.

Janice Goh
Cavenagh Law

Janice Goh is a partner in the litigation and dispute resolution practice group of Cavenagh Law (Cavenagh Law LLP and Clifford Chance Pte Ltd are registered in a formal law alliance under the name Clifford Chance Asia). She specialises in commercial dispute resolution with particular emphasis on contentious financial services regulatory advice, investigations and enforcement and white collar crime including anti-bribery.

Janice has advised on some of the most complex and high-profile cross-jurisdictional regulatory investigations in recent years, including the LIBOR/FX benchmark investigations and anti-money laundering investigations in relation to the 1Malaysia Development Berhad (1MDB) scandal.

Janice also advises regularly on employment law, and is particularly experienced in dealing with employment issues in the context of investigations.

She has been recognised by the *Singapore Business Review* as one of 'Singapore's most influential lawyers aged 40 and under'.

Janice practised in Hong Kong with Clifford Chance before moving to Singapore.

Lara Gotti
Clifford Chance

Lara Gotti practises predominantly in contentious regulatory, investigations and white-collar crime matters. She has acted for a number of companies, directors and officers and individuals on matters involving directors duties, insider trading, tax fraud, continuous disclosure obligations, bribery and corruption, data breaches and cybersecurity. She is skilled in managing large-scale litigation and routinely assists clients in responding to compulsory production notices and document reviews for internal investigations, both for domestic and multi-jurisdictional investigations.

© Law Business Research 2021

Lara is a member of the Australian Chapter of Women's White Collar Defence Association, where she holds a leadership role. She is also a member of the Access to Justice Committee for the Law Society of Western Australia.

Tim Grave
Clifford Chance

Tim Grave leads the firm's white-collar crime and anti-bribery and corruption practice in Australia. He specialises in commercial dispute resolution and related advice across a wide range of matters, including white-collar crime, regulatory investigations and enforcement, compliance investigations, competition law, sanctions advice, class actions, Corporations Act matters, directors' duties, commercial and contractual disputes and equitable claims.

Tim is recognised in *The Legal 500*, *Chambers and Partners* and *Doyle's Guide* for his work in the white-collar crime, anti-bribery, and corruption and litigation space. He is described by market sources as 'a very safe pair of hands in the regulatory space and on white-collar crime cases', and as having acted on 'some of the most significant insider trading matters'.

Kelly Hagedorn
Jenner & Block London LLP

Kelly Hagedorn is a partner in both Jenner & Block's investigations, compliance and defence practice, and data privacy and cybersecurity practice. Kelly advises on white-collar crime matters, data protection and cybersecurity matters (including data breaches) and international disputes involving fraud allegations. She has particular expertise in matters involving the financial services, gaming, hospitality and outsourcing sectors.

In 2018, Kelly was named in *Global Data Review*'s inaugural '40 under 40' list of up-and-coming professionals working in the field of data law.

Katrin Ivell
Homburger

Katrin Ivell is a partner of Homburger's white-collar and investigations team and the financial services team. She specialises in internal investigations both in the financial services sector and beyond, including when the allegation relates to sexual harassment or similar misconduct, and advises financial institutions in regulatory and compliance matters. She has conducted monitorships for the Swiss Financial Market Supervisory Authority (FINMA), advised several Swiss banks under the Swiss Bank Programme and is frequently retained in anti-bribery and corruption and anti-money laundering issues.

© Law Business Research 2021

Pamela Kiesselbach
Herbert Smith Freehills

Pamela Kiesselbach specialises in corporate crime and investigation matters, as well as disputes. She currently splits her time between Hong Kong and South East Asia, where she leads teams on some of the largest and most complex cross-border internal investigations currently under way anywhere in the world.

She has more than 20 years' experience in assisting multinational and regional clients involved in high-value, cross-border investigations and disputes involving Asian, Australian, European, UK and US companies. Pamela has broad sector experience, spanning energy companies, international and regional investment banks and other financial services providers, transport companies, manufacturers and clients in the technology and telecommunications sectors.

Pamela speaks regularly at conferences in Hong Kong and Singapore and the wider Asia-Pacific region about topics relevant to anti-corruption, cybersecurity, anti-money laundering and corporate crime.

Celeste Koeleveld
Clifford Chance

Celeste Koeleveld has more than 25 years of experience in government enforcement, regulatory and civil litigation matters that span federal, state and local government in the United States. During her career, she has held senior positions in the US Attorney's Office for the Southern District of New York (SDNY), the New York State Department of Financial Services (DFS) and the New York City Law Department. Ms Koeleveld represents clients, both corporates and individuals, with regulatory compliance, internal investigations and all phases of civil, criminal and regulatory litigation, from inception through the appellate process. Her significant government experience imparts a particularly insightful perspective to her advice and counsel in enforcement and regulatory matters.

Prior to joining Clifford Chance, Ms Koeleveld served as General Counsel at DFS, where she handled a broad spectrum of regulatory and enforcement actions, including disciplinary and enforcement proceedings. In addition, Ms Koeleveld served for 17 years in SDNY, rising to Chief of the Criminal Division, where she led a team of more than 160 Assistant US Attorneys and oversaw all criminal investigations and prosecutions. Ms Koeleveld also served for eight years as Executive Assistant Corporation Counsel at the New York City Law Department, providing legal advice to city agencies responding to government investigations from a variety of federal, state and local prosecutors and investigative bodies.

Anita Lam
Clifford Chance

Anita Lam is the head of employment, Hong Kong. Anita practises across all areas of employment law, with a particular focus on contentious employment, discrimination and data privacy disputes. As a seasoned litigator, Anita is one of very few solicitors

© Law Business Research 2021

in Hong Kong who has Higher Rights of Audience granted by the Higher Rights Assessment Board.

With over 25 years of experience in Asia, Anita is ranked independently as one of the leading employment law specialists in the region. She is listed by *The Legal 500* as a Leading Individual for Labour and Employment in Hong Kong and is ranked Band 2 by *Chambers Asia Pacific*.

Augusto Loli

Rebaza, Alcázar & De Las Casas

Augusto Loli is one of the main partners of Rebaza, Alcázar & De Las Casas, where he leads the litigation practice area. He has more than 20 years of experience as a professional attorney specialising in white-collar crime, compliance and complex corporate litigation. He has designed and implemented the defence strategies of several high-profile criminal cases involving public officials, the financial sector, telecommunications infrastructure, industry and commerce for clients from Latin America, the United States and Europe. He graduated from the National University of San Marcos and completed his master's studies in criminal law at the same university. He is a professor of white-collar criminal law at St Ignatius of Loyola University and of procedural criminal law at the University of Piura.

In addition to his private practice, he has been consulted several times by government entities, including the Advisory Committee of the Commission of Human Rights of the Congress of the Republic of Peru and the Citizen Security Commission. He is recognised by international legal publications as a leading lawyer and recommended in Peru as an expert within his field.

Hannes Lubitzsch

Noerr

Hannes Lubitzsch assists multinational companies in corporate investigations in Russian organisations concerning bribery and corruption, manipulation of tenders, violation of sanctions and other white-collar crime. He has extensive experience in assessing Russian whistleblower reports, conducting interviews on the ground, collecting and processing data in Russia, protecting and transferring investigation results, and implementing and adjusting compliance management systems in Russian organisations.

Hannes also advises multinational companies in Russia on the structuring and monitoring of business relations and transactions, including merger and acquisition transactions, taking into account liability risks for companies and management arising under Russian law and applicable foreign law, including the US Foreign Corrupt Practices Act, the UK Bribery Act and the laws of EU Member States. In addition, he advises on compliance questions arising during operations in other former Soviet republics, in particular in central Asia.

Hannes heads the compliance practice of Noerr in Russia. He has been based in Moscow since 2002.

© Law Business Research 2021

Neil McInnes
Pinsent Masons LLP

Neil McInnes, partner and barrister, is a criminal defence specialist. He has extensive experience of conducting anti-corruption and related compliance advisory work for European, UK, Asia-Pacific and multinational corporates. He regularly advises clients on the implications of the UK Bribery Act and global anti-corruption trends, as well as on fraud, money laundering and related global regulatory investigations, frequently involving multiple law enforcement agencies around the world. He has been recognised as an expert for a number of years by *Who's Who Legal* in both the business crime corporate defence and investigations categories.

Michał Magdziak
Clifford Chance

Michał Magdziak specialises in white-collar and compliance matters as well as commercial disputes (litigation and arbitration).

Michał's professional background and experience revolve mainly around criminal and regulatory proceedings. He acts as the attorney or defence counsel in white-collar criminal cases. He handles internal investigations, implementation of compliance systems, conducts training on those subjects (including dawn raids, interrogations, detention and anti-corruption issues) and advises in crisis situations.

He has worked for clients from various sectors, including energy, oil and gas, real estate and project development, construction, banking and finance, and healthcare.

Michał is the author of publications on criminal law, criminal procedure and the functioning of the justice system in Poland.

Sergio Mattos
Rebaza, Alcázar & De Las Casas

Sergio Mattos is a graduate lawyer from the University of St Martin de Porres. In 2017, he was awarded a Chevening scholarship to complete a Master of Laws degree, with a particular emphasis on criminal justice, at the London School of Economics and Political Science (United Kingdom). He also holds a master's degree, with a specialisation in criminal law, from the University of Seville (Spain), where he also completed his doctoral studies in the same field.

Sergio is a senior associate at the Lima office, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former lecturer in criminal law at the Scientific University of the South (Peru). He has also written and published several research articles focused on substantive aspects of criminal law, and he has been a speaker at a number of conferences, both in Peru and abroad.

© Law Business Research 2021

Francisca M Mok
Reed Smith LLP

Francisca Mok is the managing partner of Reed Smith's Century City office and a member of the regulatory and investigations group. She represents companies and senior individuals in government investigations by criminal and civil authorities, such as the Department of Justice and Securities Exchange Commission, in cases involving the securities laws, Foreign Corrupt Practices Act and False Claims Act. She also regularly conducts internal investigations for clients in a variety of industries, including internal investigations of alleged violations of company policy and financial fraud, and investigations, pursuant to Section 10A of the Exchange Act. Additionally, Francisca handles a variety of complex commercial litigation matters, including in the areas of securities law, unfair competition and class action litigation.

Lorena Morrone
Fornari e Associati

Lorena Morrone is a partner at Fornari e Associati, where she has been working for more than seven years as a criminal defence counsel and is particularly expert in environmental offences, offences against the public administration and serious fraud. Her clients are both individuals (charged in criminal proceedings or victims) and entities (in the event of administrative liability for an offence). In this respect, she has acquired experience in the field of internal investigations for companies, and all issues connected with it (such as reputational risk, privacy law and labour law). Therefore, her assistance is not limited to the management of criminal proceedings, but involves activities prior and subsequent to them.

Lorena is the author of articles for specialist magazines and newspapers and a co-author of the book *L'Organismo di Vigilanza nel Sistema 231*. She is a member of the European Criminal Bar Association.

Christopher J Morvillo
Clifford Chance US LLP

Christopher J Morvillo has extensive experience representing corporate and individual clients in criminal investigations and proceedings, internal investigations, and related regulatory and civil matters. With a particular focus on cross-border government and internal investigations, his many representations have involved allegations of accounting fraud, public and foreign corruption, securities fraud, insider trading, economic sanctions violations, trade secret theft and computer fraud. Mr Morvillo also advises corporations and businesses on related compliance and policy matters.

From 1999 to 2005, Mr Morvillo served as an Assistant US Attorney for the Southern District of New York, where he investigated, tried and handled appeals in a wide variety of criminal cases, including in the area of healthcare fraud, insurance fraud, money laundering, obstruction of justice, counterterrorism and narcotics. In 2005, he received the US Attorney General's Award for Exceptional Service – the Justice Department's highest award for prosecutors – in recognition of his role in the investigation and successful prosecution of a large international terrorism case.

© Law Business Research 2021

Mr Morvillo was named one of the top five most highly regarded lawyers in the United States for business crime corporate defence in the 2016 edition of *Who's Who Legal*. Mr Morvillo's expertise has also been recognised by numerous other publications, including *Chambers*, *Best Lawyers in America* and *Super Lawyers New York*. Mr Morvillo speaks and writes frequently on government investigations.

Gustavo Morales Oliver
Marval O'Farrell Mairal

Gustavo Morales Oliver is a partner at Marval O'Farrell Mairal. He joined the firm in 2006 and leads the compliance, anti-corruption and investigations practice. Gustavo also has significant experience in corporate, M&A, litigation and cross-border matters. Before joining the firm, he was in-house counsel in both the public and private sectors. He was also a foreign attorney at Yuasa and Hara Law Firm in Tokyo, Japan.

Gustavo earned a law degree from the University of Torcuato Di Tella College of Law in 2001, a specialist degree in finance from the University of San Andrés in 2009, and a Master of Laws (LLM) degree from the University of Illinois College of Law in 2010.

He teaches compliance and business law the University of Torcuato Di Tella.

He has published numerous articles with the most prestigious local and international publications and is a frequent speaker at leading universities, conferences, courses and certifications in Latin America, the United States and Europe.

Gustavo is co-director and co-author of the Compliance Treatise published by Thomson Reuters, and chairman of the Compliance Committee at Colegio de Abogados de la Ciudad de Buenos Aires.

He is a member of the Buenos Aires Bar Association and he is also admitted to the New York State Bar. Gustavo also leads Marval's annual international compliance summit.

Gustavo has been recognised as a leading practitioner by *Chambers Global*, *Chambers Latin America*, *The Legal 500* and *Who's Who Legal*.

Paweł Pogorzelski
Clifford Chance

Paweł Pogorzelski specialises in white-collar crime matters, corporate investigations and compliance, as well as commercial litigation.

Paweł regularly represents clients in law enforcement actions and criminal proceedings. He has conducted numerous investigations and related government inquiries, often cross-border in scope, concerning anti-corruption, fraud, money laundering and cybercrime. Paweł advises corporations and their boards on compliance, in addition to leading reviews of corporate compliance programmes and conducting related risk assessments. He frequently lectures and publishes articles on anti-corruption and compliance issues.

Paweł has extensive experience in representing companies in complex litigation spanning a variety of sectors, including healthcare, industrials, energy, corporate and finance.

Paweł also advises on various regulatory matters for pharmaceutical, medical device, chemical and healthcare services companies.

© Law Business Research 2021

Noel Power
Matheson

Noel Power is a senior associate in the firm's commercial litigation and dispute resolution department specialising in regulatory investigations and white-collar crime. Noel has more than 10 years' experience and recently returned from London where he was a senior associate at a US law firm. Noel advises large corporate clients, financial institutions, company directors and senior executives across a range of industries, including financial services, transport, mining and defence, on their interactions with the Serious Fraud Office, the National Crime Agency, the police and the Central Bank of Ireland. Noel focuses his practice on complex, multi-agency and cross-border investigations particularly involving international fraud, corruption and money laundering. Noel's practical experience of investigating and defending organisations and individuals has led to a compliance and advisory practice assisting national and international organisations in designing, implementing and testing effective compliance measures.

Alberto Rebaza
Rebaza, Alcázar & De Las Casas

Alberto Rebaza is the founding and managing partner of Rebaza, Alcázar & De Las Casas. As partner, he co-leads the mergers and acquisitions and corporate areas. In addition to his master's degree from the University of Virginia, he has studied at Georgetown University and in England.

Alberto has been consistently considered by legal rankings as a leading lawyer in mergers and acquisitions. He has been a speaker at conferences in Dublin, São Paulo, Bogotá, Panama City, Barcelona, New York City, Mexico City and Singapore, among others.

He has been a director for several companies and organisations, such as Edegel (energy), Rigel Peru (insurance), Liderman (services), Amrop (services), IPAE, Pesquera Alexandra (fishing) and YPO.

Very much involved in the arts world, Alberto is vice president of the Museum of Art of Lima, and a member of both the international patronage committee of the Reina de Sofia Museum and the Latin American Circle at the Guggenheim Museum in New York.

Marcus Reischl
Gleiss Lutz

Dr Marcus Reischl is a partner and a member of the compliance and investigation practice at Gleiss Lutz. Marcus advises domestic and international clients on compliance, and represents firms in court and arbitration proceedings. He specialises in strategic compliance advice as well as setting up, implementing and developing compliance structures. Marcus regularly assists companies with internal investigations for detecting irregularities, advising on their impact, in particular with regard to judicial and extrajudicial disputes with business partners and co-operation with the authorities.

© Law Business Research 2021

Marcus studied at the universities of Freiburg (Breisgau), Munich and Passau. He has been with Gleiss Lutz since 2013. In 2012, Marcus worked for an international law firm in Toronto, Canada. He is a member of the Institution of Arbitration eV (DIS) and the German Lawyers' Association (DAV). Marcus speaks German and English.

Karen Reynolds
Matheson

Karen Reynolds is a partner in the commercial litigation and dispute resolution department at Matheson and co-head of the firm's regulatory and investigations group.

Karen has a broad financial services and commercial dispute resolution practice. She has more than 10 years' experience in providing strategic advice and dispute resolution to financial institutions, financial services providers, domestic and internationally focused companies, and regulated entities and persons. She advises clients in relation to contentious regulatory matters, investigations, inquiries, compliance and governance-related matters, white-collar crime and corporate offences, commercial and financial services disputes, anti-corruption and bribery legislation, and document disclosure issues.

Karen has substantial experience in corporate restructuring and insolvency law matters, having had a lead role in some of the most high-profile corporate rescue transactions of the past 10 years. She advises liquidators, regulators, directors and insolvency practitioners in relation to corporate offences and investigations, shareholder rights and remedies, directors' duties, including in relation to fraudulent and reckless trading, and disqualification and restriction proceedings.

Flavio Romerio
Homburger

Flavio Romerio is the managing partner of Homburger and heads the white-collar and investigations team of the firm. He has extensive experience with the challenges facing Swiss clients appearing before United States courts and regulators.

Flavio Romerio represents clients in investigations by Swiss and foreign government agencies, has led large-scale internal investigations of Swiss clients and has represented them before Swiss and US regulators, including the US Department of Justice and the Office of Foreign Assets Control. Flavio Romerio regularly advises corporations and their directors and managers on all aspects of white-collar crimes.

Britt Rorrison
Meredith Connell

Britt Rorrison acts for corporate clients and government bodies as a solicitor in Meredith Connell's private litigation practice. Her clients are involved in a wide range of contract, tort and equitable claims, including claims concerning defective construction, franchising, insolvency, intellectual property and company law. She also appears in the district and high court on criminal proceedings on behalf of the Crown.

© Law Business Research 2021

She has acted for liquidators in a significant directors' duties claim currently before the high court; represented a company in claims against its auditors and former executives concerning substantial accounting irregularities; and has acted as crown counsel in district court jury trials and related appearances for criminal proceedings.

Britt has an LLB and BSc from Victoria University of Wellington.

Andrew Sackey
Pinsent Masons LLP

Andrew Sackey is a partner at Pinsent Masons. He was previously in operational command of Her Majesty's Revenue and Customs' (HMRC) Panama Papers Taskforce and, in April 2016, established and led HMRC's 500-strong Offshore, Corporate and Wealthy enforcement division. Andrew was also the responsible officer for HMRC's approach to the 'corporate criminal offence' and so is conversant with the tax administration's approach to facilitation risks and reasonable control frameworks. Andrew has also worked as a successful case controller for the Serious Fraud Office, and a Seconded National Expert in Judicial Cooperation at the Council of the European Union and so has a unique insight to a range of current high-end tax enforcement strategies. He works with peers across Pinsent Mason's contentious tax and white-collar fraud teams in both the 'prevent' and 'respond' arenas.

Sara Sanz Castillo
Uría Menéndez Abogados, SLP

Sara Sanz Castillo advises companies, their directors and employees on corporate criminal law. She has experience in criminal proceedings on a wide range of criminal offences (tax fraud, corporate criminal offences, offences against the environment and offences against workers' rights, among others). She also has experience in advising companies on the development and implementation of compliance programmes, as well as on conducting internal investigations.

María Lorena Schiariti
Marval O'Farrell Mairal

María Lorena Schiariti is a partner at Marval O'Farrell Mairal in the regulatory and administrative law team and the compliance, anti-corruption and investigations team. A specialist in administrative law, she has intervened in matters of high complexity and impact, providing comprehensive advice on issues in her areas of practice.

Owing to the wide variety of her international clients, during the past decade she has also advised on public ethics, anti-corruption and transparency policy issues, with a focus on interactions with public officials, particularly within the context of government contracts and procurement processes.

© Law Business Research 2021

Ms Schiariti holds a law degree with a specialisation in administrative law from the University of Buenos Aires, Argentina (1997) and attended the Master's in Law and Economics at the University of Torcuato Di Tella (2001–2002). She has published several articles on matters within her practice area.

She is currently a professor for the postgraduate course in compliance organised by the Instituto Argentino de la Empresa (IAE) and the Austral University.

Chambers and Partners Latin America included her as a Leading Individual (2009–2021), as Leading Lawyer by *The Legal 500* (2012–2021) and as Approved Administrative Law Private Practitioner by the Latin American Corporate Counsel Association (2014–2021). She also received the Client Choice Award, Public Law (ILO, 2018). She was included in the list of Corporate Lawyers to know and Compliance Lawyers to Know by *Latin Lawyer* (2014), 100 Women in Investigation by *Global Investigation Review* (2015) and among the best 40 Argentine lawyers under 40 by *Latin Lawyer* magazine (2003).

Judith Seddon
Ropes & Gray LLP

Judith Seddon is global co-head of Ropes & Gray's white-collar and government enforcement practice.

Judith is a leading and consistently ranked Band 1 practitioner specialising in white-collar crime, fraud, money laundering, corruption, and regulatory and criminal investigations and prosecutions. She has successfully represented corporate clients, including leading financial institutions, in some of the most significant and complex investigations mounted by the Serious Fraud Office (SFO) and Financial Conduct Authority (FCA) in the United Kingdom and by prosecuting authorities across the globe. She has successfully represented individuals in a number of the highest-profile investigations. Judith has conducted numerous internal investigations for clients involving highly sensitive matters, successfully defended clients against threatened actions by the SFO and FCA and other government agencies, and guided clients through the myriad and often unexpected challenges of navigating cross-border investigations.

Judith's professional career began at a leading specialist criminal law practice in central London led by the late Rod Fletcher. She made partner there in 2002. In 2008, she moved to a magic circle firm, where she became director in 2011 and partner in 2014; she was one of the first criminal law practitioners to join a magic circle firm, as the need for specialist criminal practitioners to deal with the growth of investigations and prosecutions of white-collar crime became essential. She joined Ropes & Gray in 2018.

Described by *Chambers* as 'excellent' and by *Who's Who Legal* as 'sharp and clever', she is acknowledged by her peers, clients and the legal press as a thoroughgoing and trenchant litigator, with an eye for detail, yet strategic, committed and indefatigable in the representation of her clients.

© Law Business Research 2021

Natalie Sherborn
Pinsent Masons LLP

Natalie Sherborn is a partner and barrister. She has extensive experience of advising both corporations and individuals facing scrutiny by law enforcement agencies and regulatory bodies. As an experienced trial lawyer, having both prosecuted and defended, Natalie is well placed to advise throughout the lifespan of a matter from pre-investigation to prosecution. She has extensive experience in devising reputational defence strategies that minimise exposure and potential risks, both pre-emptively and responsively, enabling her to counsel clients in respect of substantive issues while seeking to mitigate reputation threats.

Kabir Singh
Clifford Chance Asia

Kabir Singh is a partner in the international arbitration and dispute resolution practice of Clifford Chance. He specialises in complex cross-border disputes with a focus on India, Indonesia and South East Asia. His client roster includes large multinational corporations, international banks and financial institutions with a presence across the Asia-Pacific region.

Kabir focuses on international arbitration, regulatory investigations and contentious employment disputes. He has acted as counsel on numerous international arbitrations under the rules of ICC, SIAC, LCIA, HKIAC and AAA.

Kabir has been appointed as an alternate member of the International Court of Arbitration of the International Chamber of Commerce (the ICC Court) for a three-year term. He is a market leader and is regularly ranked by leading international legal directories such as *The Legal 500*, *Chambers and Partners* and *Who's Who Legal*. He has also been involved in various teaching initiatives, including with the ICC, SIAC, NUS Centre for International Law, Foundation for International Arbitration Advocacy and Chulalongkorn University (Thailand).

Christoph Skoupil
Gleiss Lutz

Dr Christoph Skoupil is an associated partner and a member of the compliance and investigation practice at Gleiss Lutz. Christoph advises companies on all aspects of white-collar crime and compliance. He specialises in defending companies and advising them in cases of criminal offences against the corporation. This includes both internal investigations and preventive measures.

Christoph studied at the University of Mainz. He joined Gleiss Lutz in 2015. From 2013 to 2015, Christoph worked at a leading boutique law firm specialising in white-collar crime. From 2010 to 2012, he lectured in criminal law at the University of Mainz. Christoph speaks German and English.

© Law Business Research 2021

Christian Steinle
Gleiss Lutz

Dr Christian Steinle is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Christian has considerable experience in European and international antitrust law and compliance investigations. He focuses on cartel cases and private antitrust litigation, merger control, online and distribution antitrust law, antitrust compliance programmes and internal investigations.

Christian studied in Tübingen, Fribourg (Switzerland), Bonn and Speyer. He has been a partner at Gleiss Lutz since 2008. In 2004, he was seconded as in-house counsel to a multinational group, where he specialised in international antitrust litigation. He is a member of the Association for the Study of Antitrust Law, the International Bar Association (IBA) and the American Bar Association, and belongs to the IBA Merger Working Group. Christian speaks German, English and French.

Tom Stocker
Pinsent Masons LLP

Tom Stocker is a partner at Pinsent Masons. He specialises in advising businesses on corporate criminal law, regulatory enforcement, internal investigations and compliance. Tom is qualified in Scotland and England and Wales and is ranked in Band 1 by *Chambers and Partners* for corporate crime and investigations (Scotland) and by *The Legal 500* for criminal fraud (Scotland). He has a particular specialism in corporate investigations by Police Scotland and the Crown Office and Procurator Fiscal Service, and in the operation of Scotland's corporate self-reporting and civil settlement regime. He also defends companies and individuals in regulatory enforcement cases brought by the likes of the Gambling Commission, the Financial Conduct Authority, HM Revenue and Customs, Ofgem, the Office of Financial Sanctions Implementation and the Health and Safety Executive.

Eric H Sussman
Reed Smith LLP

Eric Sussman is a partner in Reed Smith's regulatory and investigations group based in Chicago; his practice focuses on white-collar criminal defence and complex internal investigations. Eric was a deputy chief in the Financial Crimes and Special Prosecutions Unit of the United States Attorney's Office in Chicago for more than nine years and served as First Assistant State's Attorney for Cook County for 18 months. In more than two decades of practice, Eric has tried more than 35 federal and state cases, briefed and argued multiple appeals before the US Court of Appeals, and directed hundreds of investigations. Eric has handled numerous complex civil and white-collar criminal matters for corporations and executives in courts throughout the United States. Specifically, he has directed internal investigations involving the Foreign Corrupt Practices Act, the False Claims Act, insider trading issues, Dodd-Frank whistleblower provisions and healthcare fraud allegations.

© Law Business Research 2021

Tian Yi Tan
Cavenagh Law

Tian Yi Tan is a senior associate in the litigation and dispute resolution practice group of Cavenagh Law (Cavenagh Law LLP and Clifford Chance Pte Ltd are registered in a formal law alliance under the name Clifford Chance Asia).

Tian Yi advises financial institutions, banks and multinational corporations on a broad range of contentious matters. She has acted in Singapore litigation proceedings and in complex international arbitration matters. In 2019, Tian Yi was appointed Young Amicus Curiae by the Supreme Court of Singapore.

Apart from her core disputes practice, Tian Yi also advises major financial institutions and corporate clients on regulatory matters and investigations. She covers financial regulatory issues, as well as specialist areas such as employment, data privacy and healthcare.

Tian Yi graduated from the University of Oxford with first-class honours, and also holds a Master of Laws degree from Harvard Law School.

Helen Tang
Herbert Smith Freehills

Helen Tang is a partner in the Shanghai disputes practice. She has extensive experience in all forms of China-related contentious work, advising state-owned and private enterprises, as well as multinational corporations operating in China, on commercial disputes, investigations and regulatory compliance matters.

Helen obtained her LLB degree from Peking University in Beijing, and subsequently completed her graduate diploma in law studies at BPP Law School, UK, and her postgraduate certificate in laws at the University of Hong Kong. Helen previously worked in Herbert Smith Freehill's London and Hong Kong offices. She is fluent in English and is a native speaker of Mandarin and Cantonese.

Olga Tocewicz
Pinsent Masons LLP

Olga Tocewicz is a senior associate specialising in white-collar crime and corporate defence. Olga has extensive experience in advising both companies and senior individuals subject to investigation or prosecution by the UK's major law enforcement agencies in relation to allegations of financial crime, including fraud, insider trading, bribery and money laundering. Olga also provides advice in relation to the implementation of effective compliance programmes and delivers training on the topic. Olga was named as a Future Leader in Investigations in the 2020 edition of *Who's Who Legal* and also features in the 2021 edition of Global Investigations Review's 'Women in Investigations' special.

© Law Business Research 2021

Luke Tolaini
Clifford Chance

Luke Tolaini is a partner in Clifford Chance's international investigations practice. He has over 20 years' experience of investigations – many of these matters involving cross-border enforcement and related litigation. His domestic focus has been on matters involving the UK's Serious Fraud Office, Financial Conduct Authority and Competition and Markets Authority – including negotiating one of the 12 DPAs agreed to date in the United Kingdom – while his international practice has frequently involved engaging with US, European and Asian authorities on matters involving corruption, fraud, cartels, money laundering and market irregularities. He is also a lead partner in Clifford Chance's risk team, advising clients on the management and prevention of business conduct risk and crisis management. He is a member of the editorial board of Global Investigations Review.

Alexandros Tsagkalidis
Anagnostopoulos

Alexandros Tsagkalidis joined Anagnostopoulos in 2008. During his time with the firm, Alexandros has appeared in complex white-collar crime cases and gained broad experience in business crime, money laundering, asset recovery, internal investigations, financial fraud, extradition and mutual assistance requests. Alexandros was called to the Bar in 2009. He received his education at the School of Law, National University of Athens (LLB 2007, LLM in criminal law and criminal procedure, 2011). He is a member of the Legal Experts Advisory Panel of Fair Trials International and of the Hellenic Criminal Bar Association. Alexandros has published in Greek and English on matters of asset recovery, investigation procedures, business crimes, extradition and defence rights in the European Union.

Heloísa Barroso Uelze
Trench Rossi Watanabe

Heloísa Barroso Uelze joined the firm in 2000 and became a partner in 2005. She is currently the head of the Brazilian public law, government relations and regulatory, and ethics, compliance and investigations practice groups. Mrs Uelze has vast experience of working in compliance matters, representing clients both before public administration and the judiciary department. On numerous occasions she has dealt with the federal and state public prosecutors' offices in negotiating deals in matters that involved Brazil's Improbity Law and Anti-Corruption Law. She has also defended clients' interests before several courts of accounts (at federal, state and municipal levels). Mrs Uelze also works with clients in strengthening their compliance areas, by improving both the internal rules and the mechanisms to enforce those rules. She prepares and reviews internal policies and guidelines, and also provides speeches and training to clients' teams, to make sure everyone is aware of the applicable rules.

Mrs Uelze is recognised as a leading practitioner in the above-mentioned areas of law by various international listings, such as Chambers and Partners, LACCA, *Análise Advocacia* and *PLC*. She graduated from the Pontifical Catholic University of São Paulo

© Law Business Research 2021

Law School and is a specialist in administrative law, constitutional law, tax law and civil procedure.

Alex van Weezel
Claro y Cia

Alex van Weezel is a partner at Claro y Cia, where he focuses on litigation and arbitration, white-collar crime, administrative penalties and antitrust. His practice areas are criminal, litigation, data protection and cybersecurity, administrative law, administrative procedural law and constitutional matters. He joined the firm in 2006.

He is professor of criminal law at the Pontifical Catholic University of Chile and the University of Chile. He also teaches PhD and postgraduate programmes and participates as relator in programmes of specialisation focused on participants in the criminal procedural system in Chile and abroad. Further, he is the author of several books and numerous articles about criminal law, criminal procedure and theory of law, especially on white-collar crime, regulated markets and the liability arising therefrom.

Alex van Weezel has a PhD from the University of Bonn (DAAD Scholarship, 2005) and gained his JD from the Pontifical Catholic University of Chile in 1993.

Alex van Weezel is a member of the Chilean Bar and the Criminal Sciences Institute.

Donna Wacker
Clifford Chance

Donna Wacker is the co-head of Clifford Chance's Asia Pacific regulatory practice and the head of both the Hong Kong contentious regulatory and contentious insolvency practices. She is admitted in Hong Kong, Australia and England and Wales and has been practising in Asia since 1999.

Donna specialises in regulatory enforcement investigations and advice in the financial sector, as well as dispute resolution for financial services firms, particularly complex, cross-border disputes. She has represented financial institutions, intermediaries, funds and corporates on a range of regulatory issues and investigations (such as insider dealing, misuse of confidential information, market manipulation, mis-selling of derivatives, electronic trading issues, mismarking of trading books, conflict of interest and breaches of reporting obligations), as well as complex litigation (including mis-selling claims and derivatives litigation), and insolvency issues and resolution.

Donna is ranked highly by *Chambers and Partners* for litigation and contentious regulatory work. She is similarly well regarded by *The Legal 500*, *IFLR 1000* and is recognised as a Global Leader for Investigations by *Who's Who Legal*. She is the chairperson of the Hong Kong Law Society's Overseas Lawyers Qualification Committee and a founding member of the International Women's Insolvency and Restructuring Confederation, Hong Kong Chapter.

© Law Business Research 2021

Michael Wang
Clifford Chance

Michael Wang is a consultant in Clifford Chance's Hong Kong litigation and dispute resolution practice. Admitted in Hong Kong in 2012, Michael is a native Mandarin speaker and is fluent in Cantonese.

Michael advises on a broad range of contentious regulatory matters and complex banking and commercial litigation. He regularly advises banks, investment funds, brokerages, asset managers and listed companies in a wide range of regulatory investigations and compliance issues, including market misconduct and manipulation, sponsor liability, electronic trading, reporting failures, insider dealing, operation of alternative liquidity pool, position limits reporting, facilitation trading, financial resources rules and listing rules compliance.

Michael also advises and represents banks and high net worth individuals in a number of high-profile court and tribunal hearings, both local and cross-border, involving mis-selling of structured products and general commercial disputes.

Michael is recognised by *Who's Who Legal* 2021 as a Future Leader in Investigations and by *The Legal 500*, with clients praising him as 'excellent' and someone 'who executes everything flawlessly'. He is also commended as 'clever, hardworking and prepared to roll up [his] sleeves' (*The Legal 500* 2021, *Dispute Resolution: Litigation*, China).

Kyle Wombolt
Herbert Smith Freehills

Kyle Wombolt is the global head of Herbert Smith Freehills' corporate crime and investigations practice. He has been described by clients as 'one of the cornerstones of investigations work in Asia' and 'an exceptional lawyer'. Based in Hong Kong, Kyle has 20 years' experience in Asia and has led investigations and compliance projects in more than 40 countries worldwide. He focuses on multi-jurisdictional anti-corruption, regulatory, fraud and accounting investigations, as well as trade and sanctions issues involving multinational and major regional corporates. He has extensive experience in dealing with a broad group of government agencies and regulators in key jurisdictions in Asia, Europe, Australia and the United States.

Kyle also has a diverse range of experience in implementing anti-corruption compliance programmes for a broad range of clients, including investment banks and other financial institutions and multinational companies. He regularly advises clients on corruption risks associated with a wide range of transactions, including initial public offerings, mergers and acquisitions, and joint ventures.

Kyle is admitted to practise in Hong Kong, California and New York, and is a registered foreign lawyer in England and Wales.

© Law Business Research 2021

Jonathan Wong
Clifford Chance

Jonathan Wong is a partner in Clifford Chance's litigation and dispute resolution practice in Hong Kong. He has a broad practice spanning regulatory and internal investigations, cross-border litigation and arbitration.

Having trilingual capabilities (English, Mandarin and Cantonese), Jonathan advises a wide range of international and Chinese banks, insurers and corporates on the full spectrum of regulatory investigations and financial crime matters. His work includes leading on investigations into the role and conduct of sponsors of Hong Kong initial public offerings, allegations of commodities price-fixing, insider dealing, control failures, market misconduct, data breaches and listed compliance.

Jonathan is admitted as a solicitor in Hong Kong and is an advocate and solicitor in Singapore.

William Wong
Clifford Chance

William Wong is a Hong-Kong based consultant in Clifford Chance's litigation and dispute resolution practice. He is admitted in Hong Kong and England and Wales, and he has more than 15 years of experience in financial services litigation, white-collar crime and all aspects of contentious regulatory work, and he regularly advises a broad range of institutional clients (investment banks, private banks, insurance companies, hedge funds and asset managers) and individual clients (senior executives of listed corporations and financial institutions) in local and cross-border regulatory investigations. He also advises on technology-related risk issues and commercial litigation from time to time.

Before joining Clifford Chance, William had held in-house positions at two bulge-bracket investment banks, advising on their regulatory and compliance issues and internal investigations.

With his in-house experience and trilingual capability, William is a popular counsel of choice, particularly when clients require first-class advice and Chinese language support. He is recognised by *Who's Who Legal* 2021 as a Future Leader in Investigations, a Next Generation Lawyer in Litigation by *The Legal 500 Asia Pacific* in 2019 and is noted in the 2021 edition of *The Legal 500* as a 'seasoned professional' with 'excellent compliance related skills and techniques to deal with regulators'.

Matthew Worby
Jenner & Block London LLP

Matthew Worby is an associate in Jenner & Block's investigations, compliance and defence practice group. Matthew has experience of representing both international corporates in investigations and defending individuals against prosecution by the Serious Fraud Office.

© Law Business Research 2021

Jerina Zapanti
Anagnostopoulos

Jerina (Gerasimoula) Zapanti is a member of the Athens Bar (2001) and the Hellenic Criminal Bar Association (2007). She has considerable experience in cross-border cases involving fraud, bribery, cartel offences, tax offences and money laundering. She is very active in internal corporate investigations and risk management assessment for national and multinational corporations.

María Haydée Zegarra
Rebaza, Alcázar & De Las Casas

María Haydée Zegarra leads the labour and employment law practice and has extensive experience in providing legal counselling on personnel hiring and lay-offs, collective bargaining, outsourcing of workforces, implementation of internal policies and internal investigations for companies in the fishing, port industry, telecommunications, financial, insurance, agro-industrial and aeronautical sectors.

She has been highlighted by clients for the preparation of strong defence strategies in relation to judicial processes and administrative inspections thanks to her knowledge of clients' operational know-how and more than 15 years of experience in the labour field.

María Haydée actively participates in training workshops for companies on labour issues, such as employment modalities, management of overtime working, disciplinary sanctions management and employment of foreign employees, among other things.

Julie Zorrilla
Navacelle

Julie Zorrilla has worked for more than eight years on complex cross-border financial and criminal matters, including asset recovery, embargo and index manipulation (LIBOR and SSA), involving top executives of global foreign and French financial institutions.

Julie handles large-scale corruption and compliance matters, advising on both legal and crisis management for corporations with global operations. She is involved in assisting Stéphane de Navacelle in connection with his appointment as expert pursuant to a World Bank negotiated resolution agreement.

She also participates in determining the strategy for and the implementation of internal investigations.

Julie became counsel at Navacelle in 2019 and partner in 2020. Prior to joining Navacelle in 2012, she worked in the Legal Affairs Department of the Ministry of the Economy and Finance in 2012 and as a trainee auditor at the Paris Court of Appeal in 2011. Julie graduated from Paris X University and from the Institute of Criminal Sciences at University Paris II Panthéon-Assas (2010).

© Law Business Research 2021

Appendix 2

Contributors' Contact Details

Anagnostopoulos

6, Patriarchou Ioakeim
106 74 Athens
Greece
Tel: +30 210 729 2010
Fax: +30 210 729 2015
ianagnostopoulos@iag.gr
jzapanti@iag.gr
atsagkalidis@iag.gr
www.iag.gr

Blank Rome LLP

1271 Avenue of the Americas
New York, NY 10020
United States
Tel: +1 212 885 5196
Fax: +1 212 885 5001
jennifer.achilles@blankrome.com
www.blankrome.com

Claro y Cia

Avenida Apoquindo 3721, Piso 14
Las Condes
Santiago 755 0177
Chile
Tel: +562 2367 3000
avanweezel@claro.cl
sbreton@claro.cl
www.claro.cl

Clifford Chance

Level 7, 190 St George's Terrace
Perth, WA 6000
Australia
Tel: +61 8 9262 5555
lara.gotti@cliffordchance.com

Level 16, 1 O'Connell Street
Sydney, NSW 2000
Australia
Tel: +61 2 8922 8000
tim.grave@cliffordchance.com

© Law Business Research 2021

27th Floor, Jardine House
One Connaught Place
Hong Kong
Tel: +852 2825 8888
Fax: +852 2825 8800
donna.wacker@cliffordchance.com
jonathan.wong@cliffordchance.com
anita.lam@cliffordchance.com
william.wong@cliffordchance.com
michael.wang@cliffordchance.com

Norway House
ul. Lwowska 19
00-660 Warsaw
Poland
Tel: +48 22 627 11 77
marcin.cieminski@cliffordchance.com
pawel.pogorzelski@cliffordchance.com
monika.diehl@cliffordchance.com
michal.magdziak@cliffordchance.com

Clifford Chance Asia*
Marina Bay Financial Centre
25th Floor, Tower 3
12 Marina Boulevard
Singapore 018982
Tel: +65 6410 2200
kabir.singh@cliffordchance.com
janice.goh@cliffordchance.com
tianyi.tan@cliffordchance.com
www.cavenaghlaw.com
* Clifford Chance Asia is a formal law alliance in Singapore between Clifford Chance Pte Ltd and Cavenagh Law LLP

Clifford Chance LLP
10 Upper Bank Street
Canary Wharf
London, E14 5JJ
United Kingdom
Tel: +44 20 7006 1000
Fax: +44 20 7006 5555
luke.tolaini@cliffordchance.com

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
christopher.morvillo@cliffordchance.com
celeste.koeleveld@cliffordchance.com

www.cliffordchance.com

Cravath, Swaine & Moore LLP

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
United States
Tel: +1 212 474 1000
Fax: +1 212 474 3700
jburetta@cravath.com
www.cravath.com

Fornari e Associati

Via Chiossetto 18
20122 Milan
Italy
Tel: +39 02 541 222 06
e.difiorino@fornarieassociati.com
l.morrone@fornarieassociati.com
www.fornarieassociati.com

Fountain Court Chambers

Fountain Court
Temple
London, EC4Y 9DH
United Kingdom
Tel: +44 20 7583 3335
Fax: +44 20 7353 0329
eld@fountaincourt.co.uk
www.fountaincourt.co.uk

© Law Business Research 2021

Gleiss Lutz

Taunusanlage 11
60329 Frankfurt
Germany
Tel: +49 69 95514 0
Fax: +49 69 95514 198
eike.bicker@gleisslutz.com
christoph.skoupil@gleisslutz.com
marcus.reischl@gleisslutz.com

Lautenschlagerstraße 21
70173 Stuttgart
Germany
Tel: +49 711 8997 0
Fax: +49 711 855096
christian.steinle@gleisslutz.com

www.gleisslutz.com

Herbert Smith Freehills

Herbert Smith Freehills LLP
38th Floor, Bund Centre
222 Yan An Road East
Shanghai 200002
China
Tel: +86 21 2322 2000
Fax: +86 21 2322 2322
helen.tang@hsf.com
tracey.cui@hsf.com

23rd Floor, Gloucester Tower
15 Queen's Road Central
Hong Kong
Tel: +852 2845 6639
Fax: +852 2845 9099
kyle.wombolt@hsf.com
pamela.kiesselbach@hsf.com

www.herbertsmithfreehills.com

Homburger

Prime Tower
Hardstrasse 201
8005 Zurich
Switzerland
Tel: +41 43 222 10 00
Fax: +41 43 222 15 00
flavio.romerio@homburger.ch
claudio.bazzani@homburger.ch
katrin.ivell@homburger.ch
reto.ferrari-visca@homburger.ch
www.homburger.ch

Jenner & Block London LLP

Level 17, Tower 42
25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Tel: +44 33 0060 5400
Fax: +44 33 0060 5499
rdalling@jenner.com
khagedorn@jenner.com
mworby@jenner.com
www.jenner.com

Marval O'Farrell Mairal

Avenida Leandro N. Alem 882
C1001AAQ Buenos Aires
Argentina
Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
glo@marval.com
mls@marval.com
www.marval.com

© Law Business Research 2021

Matheson

70 Sir John Rogerson's Quay
Dublin 2, D02 R296
Ireland
Tel: +353 1 2322387
karen.reynolds@matheson.com
connor.cassidy@matheson.com
noel.power@matheson.com
www.matheson.com

Meredith Connell

Level 7, MC Centre
8 Hardinge Street
Auckland 1010
New Zealand
Tel: +64 9 336 7500
william.fotherby@mc.co.nz
brittany.rorrison@mc.co.nz
caitlin.anyon-peters@mc.co.nz
www.mc.co.nz

Navacelle

60 rue Saint-Lazare
75009 Paris
France
Tel: +33 1 48 78 76 78
sdenavacelle@navacellelaw.com
jzorrilla@navacellelaw.com
www.navacelle.law

Noerr

1-ya Brestskaya ul. 29
125047 Moscow
Russia
Tel: +7 495 7995696
Fax: +7 495 7995697
hannes.lubitzsch@noerr.com
www.noerr.com

Outer Temple Chambers

222 Strand
London, WC2R 1BA
United Kingdom
Tel: +44 20 7353 6381
Fax: +44 870 220 3256
michael.bowesqc@outertemple.com
www.outertemple.com

Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Carrera 9 #74-08
Office 105
Bogotá
Colombia
Tel: +571 3268600
Fax: +571 3268610
pamela.alarcon@ppulegal.com
www.ppulegal.com

Pinsent Masons LLP

The Soloist Building
1 Lanyon Place
Belfast, BT1 3LP
United Kingdom
Tel: +44 28 9089 4800
laura.gillespie@pinsentmasons.com

30 Crown Place
Earl Street
London, EC2A 4ES
United Kingdom
Tel: +44 20 7418 7000
Fax: +44 20 7418 7050
tom.stocker@pinsentmasons.com
neil.mcinnes@pinsentmasons.com
natalie.sherborn@pinsentmasons.com
andrew.sackey@pinsentmasons.com
olga.tocewicz@pinsentmasons.com

www.pinsentmasons.com

© Law Business Research 2021

Rebaza, Alcázar & De Las Casas

Via Principal 133, 2nd and 3rd Floors
Edificio Real Dos
San Isidro
Lima 27
Peru
Tel: +511 442 5100
Fax: +511 442 5100 237
alberto.rebaza@rebaza-alcazar.com
augusto.loli@rebaza-alcazar.com
hector.gadea@rebaza-alcazar.com
mariahaydee.zegarra@rebaza-alcazar.com
sergio.mattos@rebaza-alcazar.com
www.rebaza-alcazar.com

Reed Smith LLP

10 South Wacker Drive
40th Floor
Chicago, IL 60606-7507
United States
Tel: +1 312 207 1000
Fax: +1 312 207 6400
esussman@reedsmith.com
bbolerjack@reedsmith.com

1901 Avenue of the Stars
Suite 700
Los Angeles, CA 90067-6078
United States
Tel: +1 310 734 5200
Fax: +1 310 734 5299
fmok@reedsmith.com

www.reedsmith.com

Ropes & Gray LLP

60 Ludgate Hill
London, EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
judith.seddon@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
ama.adams@ropesgray.com
maria.calvet@ropesgray.com

www.ropesgray.com

Trench Rossi Watanabe

Rua Arq. Olavo Redig de Campos, 105
31º andar
Edifício EZ Towers, Torre A
São Paulo 04711-904
Brazil
Tel: +55 11 3048 6800/5506 3455
heloisa.uelze@trenchrossi.com
felipe.ferenzini@trenchrossi.com
joao.gameiro@trenchrossi.com
www.trenchrossi.com

Uría Menéndez Abogados, SLP

C/ Príncipe de Vergara, 187
Plaza de Rodrigo Uría
28002 Madrid
Spain
Tel: +34 915 860 400
jaime.alonso@uria.com
sara.sanz@uria.com
www.uria.com

© Law Business Research 2021

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-272-5

© Law Business Research 2021