Global Investigations Review

The Practitioner's Guide to Global Investigations

Second Edition

Editors
Judith Seddon, Clifford Chance
Eleanor Davison, Fountain Court Chambers
Christopher J Morvillo, Clifford Chance
Michael Bowes QC, Outer Temple Chambers
Luke Tolaini, Clifford Chance

2018

The Practitioner's Guide to Global Investigations

Second Edition

Editors:

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

GIR

Global Investigations Review

Publisher
David Samuels

Senior Co-Publishing Business Development Manager
George Ingledew

Project Manager
Edward Perugia

Editorial Coordinator
Iain Wilson

Head of Production
Adam Myers

Senior Production Editor
Simon Busby

Copy-editor
Jonathan Allen

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

ISBN 978-1-912377-34-3

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

Acknowledgements

ALLEN & OVERY LLP

ANAGNOSTOPOULOS

ARCHER & ANGEL

BAKER McKENZIE LLP

BANQUE LOMBARD ODIER & CO LTD

BARCLAYS BANK PLC

BCL SOLICITORS LLP

BDO USA, LLP

BROWN RUDNICK LLP

BRUNSWICK GROUP LLP

CADWALADER, WICKERSHAM & TAFT LLP

CLIFFORD CHANCE

CLOTH FAIR CHAMBERS

CORKER BINNING

DEBEVOISE & PLIMPTON LLP

DECHERT LLP

DREW & NAPIER LLC

FOUNTAIN COURT CHAMBERS

FOX WILLIAMS LLP

FRESHFIELDS BRUCKHAUS DERINGER

GIBSON, DUNN & CRUTCHER LLP

GOODWIN

HERBERT SMITH FREEHILLS

HOGAN LOVELLS

KINGSLEY NAPLEY LLP

KNOETZL

MATHESON

NAVACELLE

NOKIA CORPORATION

NORTON ROSE FULBRIGHT

OUTER TEMPLE CHAMBERS

PINSENT MASONS LLP

PROSKAUER ROSE LLP

QUINN EMANUEL URQUHART & SULLIVAN, LLP

RICHARDS KIBBE & ORBE LLP

ROPES & GRAY LLP

RUSSELL McVEAGH

SCHELLENBERG WITTMER LTD

SIMMONS & SIMMONS LLP

SKADDEN, ARPS, SLATE, MEAGHER & FLOM (UK) LLP

SOFUNDE OSAKWE OGUNDIPE & BELGORE

SULLIVAN & CROMWELL LLP

WILLKIE FARR & GALLAGHER (UK) LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

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.

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

It will be published annually as a single volume and is also available online, as an e-book and in PDF format.

The volume

This book is in two parts.

Part 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 approach and thought processes of those who are at the cutting edge of this work, on the basis that others can learn much from their approach, and there is a read-across to the position elsewhere.

Part I is then complemented by Part II's granular look at the detail of various jurisdictions, highlighting among other things where they vary from the norm.

Online

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

The publisher would like to thank the editors for their exceptional energy and vision in putting this project together. Together we welcome any comments or suggestions from readers on how to improve it. Please write to us at:
co-publishing@globalinvestigationsreview.com.

Contents

PART II
GLOBAL INVESTIGATIONS AROUND THE WORLD

Preface

The history of the global investigation

Over the past decade, the number and profile of multi-agency, multi-jurisdictional regulatory and criminal investigations have risen exponentially. Naturally, this global phenomenon exposes corporations and their employees to greater risk of potentially hostile encounters with foreign law enforcement authorities and regulators than ever before. This is partly owing to the continued globalisation of commerce, as well as the increasing enthusiasm of some prosecutors to use expansive theories of corporate criminal liability to extract exorbitant penalties against corporations 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, both direct and collateral, for individuals and businesses are of unprecedented magnitude.

The guide

To aid practitioners faced with the myriad and often unexpected challenges of navigating a cross-border investigation, this book brings together for the first time the perspectives of leading experts from across the globe.

The chapters that follow in Part I of the guide cover in depth the broad spectrum of the law, practice and procedure applicable to cross-border investigations in both the United Kingdom and United States. Part I tracks the development of a serious allegation (whether originating from an internal or external source) through its stages of development, considering the key risks and challenges as matters progress; it provides expert insight into the fact-gathering stage, document preservation and collection, witness interviews, and the complexities of cross-border privilege issues; and it discusses strategies to successfully resolve cross-border probes and manage corporate reputation throughout an investigation.

In Part II of the book, local experts from national jurisdictions respond to a common 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 law and practice evolved. For this second edition we have revised the chapters to reflect recent developments. In the United Kingdom, some eagerly awaited English court decisions have raised significant legal privilege implications, and new corporate offences related to tax evasion have been introduced. In the United States, despite a new administration, the FCPA's enhanced enforcement project – the Pilot Program – has been extended. We have also included substantive chapters covering extraterritoriality considerations from both the US and UK perspectives. Further, Part II now covers 16 jurisdictions, including China and Nigeria, and we expect subsequent editions to have an even broader jurisdictional scope.

The Practitioner's Guide to Global Investigations has been designed for external and in-house legal counsel; compliance officers and accounting practitioners who wish to benchmark their own practice against that of leaders in the fields; and prosecutors, regulators and advisers operating in this complex environment.

Acknowledgements

The Editors gratefully acknowledge the insightful contributions of the following lawyers from Clifford Chance: Chris Stott, Zoe Osborne and Oliver Pegden in London; Megan Farrell, Jayla Jones, Delphine Miller, Amy Montour and Mary Jane Yoon in New York; and Hena Schommer and Michelle Williams in Washington, DC.

The Editors would also especially like to thank Clifford Chance lawyers Tara McGrath (who went above and beyond to bring this book together) and Kaitlyn Ferguson for their significant contributions.

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini
November 2017
London and New York

Part I

Global Investigations in the United Kingdom and the United States

11

Production of Information to the Authorities

Hector Gonzalez, Rebecca Kahan Waldman, Caroline Black and William Fotherby[1]

Introduction 11.1

There are many situations in which a company may face a choice, or a demand, to disclose documents and information to a law enforcement authority or regulator, ranging from responding to a raid on corporate and individual premises, to compliance with a subpoena or other compulsory process, to the voluntary provision of information during a self-disclosure. The types of information and the circumstances in which a company is obliged – or even able – to produce relevant documents is circumscribed by various laws. For example, a company must address concerns regarding confidentiality, employee privacy, data protection and legal privilege (and, in certain jurisdictions, bank secrecy restrictions or blocking statutes). This becomes additionally complicated in cross-border cases where multiple legal regimes may apply and may conflict with one another. Add to this the not uncommon scenario of authorities from different countries seeking the same (or slightly different) information and it becomes a legal and practical minefield. This chapter cannot hope to cover the immense number of variables that a company may face in these circumstances, but it does seek to provide practical guidance on some of the most important points.

1 Hector Gonzalez, Rebecca Kahan Waldman and Caroline Black are partners, and William Fotherby is an associate, at Dechert LLP.

11.2 Production of documents to the authorities

11.2.1 Formal requests for disclosure (and related document hold issues)

11.2.1.1 Commonly used powers (UK)

Most regulatory and enforcement authorities have formal powers to compel individuals and companies to produce documents and provide information.

In the area of financial crime and corruption involving the United Kingdom, the most likely authority to be seeking to investigate and prosecute will be the Serious Fraud Office (SFO). It has powers to seek the production of documents and information at both a pre-investigation stage in relation to corruption cases under section 2A of the Criminal Justice Act 1987, and, once it opens a formal investigation, under section 2 of the same Act. These powers can be exercised against companies and individuals to produce documents and information, including by way of compelled interview where there is no right to silence (although the individual cannot be later prosecuted regarding matters arising from the interview, unless the information is found to be false). A failure to provide the documents and information within the time specified in the production notice is a criminal offence, unless the recipient can show that it had a reasonable excuse not to comply (such as an injunction preventing production).

In the field of financial markets regulation, the Financial Conduct Authority (FCA) has powers to compel the production of documents, contained in Part 11 of the Financial Services and Markets Act 2000 (FSMA). The key provision is section 165, which is set out here as an example of how information-gathering powers are conferred:

> *165 Authority's power to require information: authorised persons etc.*
> *(1) The Authority may, by notice in writing given to an authorised person, require him–*
> *(a) to provide specified information or information of a specified description; or*
> *(b) to produce specified documents or documents of a specified description.*
> *(2) The information or documents must be provided or produced–*
> *(a) before the end of such reasonable period as may be specified; and*
> *(b) at such place as may be specified.*
> *(3) An officer who has written authorisation from the Authority to do so may require an authorised person without delay–*
> *(a) to provide the officer with specified information or information of a specified description; or*
> *(b) to produce to him specified documents or documents of a specified description.*
> *(4) This section applies only to information and documents reasonably required in connection with the exercise by the Authority of functions conferred on it by or under this Act.*
> *(5) The Authority may require any information provided under this section to be provided in such form as it may reasonably require.*

(6) The Authority may require–

(a) any information provided, whether in a document or otherwise, to be verified in such manner, or

(b) any document produced to be authenticated in such manner, as it may reasonably require.

'Authorised person' is defined in section 31 of FSMA and means, very broadly, a person providing a regulated financial service.

The FCA has set out its policy in relation to its exercise of enforcement powers under the FSMA (and other legislation) in its Enforcement Guide.[2] The Enforcement Guide is useful as it not only sets out the FCA's approach to its task as the United Kingdom's financial markets regulator, but also it reflects the general approach of UK regulators to their document production powers.

In paragraphs 4.8 and 4.9 of the Enforcement Guide, the FCA states that its standard practice is to use its statutory powers to require the production of documents, the provision of information or the answering of questions in interview. The FCA suggests that this is for reasons of fairness, transparency and efficiency. The Enforcement Guide goes on to suggest, however, that it will sometimes be appropriate to depart from this standard practice, as it relates to document production, in cases:

- involving third parties with no professional connection with the financial services industry, such as the victims of an alleged fraud or misconduct, in which case, the FCA will usually seek information voluntarily;
- where the FCA has been asked by an overseas or EEA regulator to obtain documents on their behalf, in which case the FCA will discuss with the overseas regulator the most appropriate approach.

In the second scenario, it is important to consider the effect of regimes and jurisdictional protections colliding. For example, how might the US right to silence mesh with the UK compelled disclosure regime? The Enforcement Guide states that the FCA will make it clear to the company or individual concerned whether it requires him, her or it to produce information or answer questions under FSMA or whether the provision of information is voluntary.[3] See Chapters 15 to 18 on representing individuals in interviews and in cross-border proceedings.

Similar (but unique) powers also lie in the hands of the Competition and Markets Authority, the National Crime Agency, police, Her Majesty's Revenue and Customs, and the Health and Safety Executive. Many of these authorities may also apply for and obtain search warrants and use these powers more often than their US counterparts do.

See Section 11.3

2 Financial Conduct Authority, Enforcement Guide (January 2016).

3 Whether the FCA compels testimony from an individual can have an impact on whether that information can be used in connection with a criminal proceeding in the United States. Recently, the Second Circuit Court of Appeals held that testimony compelled by the FCA cannot be used against a defendant in a criminal prosecution. See *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017).

11.2.1.2 Commonly used powers (US)

In the United States, most federal agencies, including the United States Department of Justice (DOJ), the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC), may issue subpoenas (or administrative orders) and compel individuals and companies to produce documents and testimony.[4] In the case of the DOJ, a subpoena may compel the production of documents in connection with either a civil or criminal investigation.[5] The CFTC's regulations provide that:

> *The Commission or any member of the Commission or of its staff who, by order of the Commission, has been authorized to issue subpoenas in the course of a particular investigation may issue a subpoena directing the person named therein to appear before a designated person at a specified time and place to testify or to produce documentary evidence, or both, relating to any matter under investigation.*[6]

Additionally, state agencies and each state's attorney general can compel the production of documents and testimony. As an example, Section 352 of the New York General Business Law permits the attorney general to commence an investigation of an individual or corporation and to seek documents and testimony in connection with that investigation. The Securities Act, the Securities Exchange Act, the Investment Advisers Act, and the Investment Company Act all permit the SEC to issue subpoenas in connection with an ongoing investigation of misconduct.[7] Before a subpoena can be issued, the staff of the SEC must obtain a formal order of investigation.[8]

Criminal offences for refusing to comply with a request, providing false or misleading statements, or concealing documents, generally supplement such powers.[9]

---

4 Other federal agencies such as the Consumer Financial Protection Bureau and the Federal Trade Commission are authorised to issue subpoenas. Other agencies are required to seek the assistance of the United States Attorney's Office in seeking documents and testimony. For a discussion of the use of administrative subpoenas, see https://www.justice.gov/archive/olp/rpt_to_congress.htm#f23.

5 For information regarding criminal matters, see Section 9-13 of the U.S. Attorneys' Manual (USAM). The Civil Division is authorised to issue subpoenas by a number of statutes.

6 17 C.F.R. § 11.4(a).

7 Section 19(c) of the Securities Act of 1933, 15 U.S.C. § 77s(c); Section 21(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78u(b); Section 209(b) of the Investment Advisers Act of 1940, 15 U.S.C. § 80b–9(b); and Section 42(b) of the Investment Company Act of 1940, 15 U.S.C. § 80a–41(b).

8 For information regarding procedures for obtaining a formal order of investigation, see sections 2.2.3-2.3.4 of the Enforcement Manual of the Securities and Exchange Commission Division of Enforcement, available at https://www.sec.gov/divisions/enforce/enforcementmanual.pdf (4 June 2015).

9 18 U.S.C. §§ 401, 1001; see also 7 U.S.C. §§ 9, 13(a)(3). Rule 17 of the Federal Rules of Criminal Procedures, governs subpoenas, including grand jury subpoenas and Rule 17(g) authorises federal courts to exercise its contempt powers for non-compliance ('The court (other

Scope and timing 11.2.1.3

In practice, a company can do little to resist complying with a formal request for disclosure without resorting to court proceedings to challenge the validity or scope of the request. However, it can likely negotiate with the relevant authority regarding the scope of documents responsive to the request and the production date to limit the scope of the request to what is proportionate and reasonable.

Broadly drawn requests are unfortunately not uncommon, as investigators seek to ensure the requests will capture all relevant information. Early engagement with the relevant authority will typically ensure that both parties can agree on scope and a timetable for production: a request looking back over a long period, or even without any time limit, could involve a time- and resource-intensive review and expensive production exercise. This may not be in the interests of the prosecuting agency or the company if a more targeted request could produce the information. Whether an agreement to narrow the scope of the request is possible is likely to depend, in large part, on factors outside the company's control – such as the nature and scope of the authority's investigation (which the authority may be unwilling to share and is likely to base on information and evidence outside the company's knowledge). However, the company and its legal advisers should nonetheless seek a reasonable, proportionate and practically achievable production: for example, by seeking to agree to produce documents relating to X project, between Y–Z dates and if necessary to produce the documents in tranches.

It becomes increasingly difficult to manage the response to multiple authorities particularly if they are in different countries and have different areas of focus. Similarly, a company must consider whether the production notice extends to materials held overseas.

See Section 11.2.3

See Section 11.2.4

Practical steps on receipt 11.2.1.4

Upon receipt of a document request, a company should immediately issue a document retention (or hold) notice (DRN) (if one is not already in place). The issuing of a DRN will assist the company to demonstrate that it has taken steps to preserve all potentially relevant documents in existence at the date of the request. The DRN should track the terms of the production notice, and be sent to all personnel who may have responsive documents, including the IT department and records department. The term 'document' should be widely drawn to include any paper or electronic records present on any media belonging to the company or its employees, including corporate information located off-site. The company may also need to manage complicated issues around data privacy and personal media.

See Chapters 13 and 14 on employee rights

The DRN should confirm that employees must not delete, alter, conceal or otherwise destroy company documents. Simultaneously, the company should take steps to secure and preserve all relevant information held on the company's servers

than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district.').

and back-up tapes, including through external providers. It should also immediately suspend routine document and data destruction processes.

Most authorities will have their own technical standards, which the collection and production of electronically stored information must meet. It is therefore likely that a company seeking to respond to a subpoena or production notice will want to consider instructing a forensic IT specialist company to assist with the collection and production efforts. This will have the added benefit of ensuring that a company can demonstrate the independence of this analysis, that it is taking clear co-operative steps, and protects employees, as far as possible, from having to give evidence in any subsequent proceedings.

11.2.2 Informal requests for disclosure: voluntary production and co-operation

A company may wish to consider voluntarily providing documents to an authority as part of a self-report or to demonstrate its co-operation with an investigation. Government investigators and investigating authorities regularly hold out the possibility of co-operation credit to companies to encourage them to provide information about their own misconduct.

From February 2014, deferred prosecution agreements (DPAs) have been available in the United Kingdom to the SFO and Crown Prosecution Service (CPS) for disposing of corporate criminal conduct relating broadly to economic crime (including, in particular, fraud, corruption and money laundering).[10] The current Director of the SFO, David Green QC, and the English courts have emphasised that one of the most important factors for a DPA is early reporting and co-operation by the company. Co-operation should be 'genuinely proactive'.[11] This includes the voluntary production of relevant documents, the importance of which has been demonstrated in the recent DPA case of *SFO v. Rolls-Royce PLC*,[12] discussed later in this chapter.

In the United States, too, the authorities have routinely emphasised that they will consider self-reporting and co-operation with government investigations as a key factor when determining whether to charge a corporation.[13] Under the DOJ's FCPA Pilot Program,[14] 'for a company to receive credit for volun-

10 DPAs were introduced by s.45 and Sch. 17 of the Crime and Courts Act 2013.

11 Crown Prosecution Service and Serious Fraud Office, Deferred Prosecution Agreements Code of Practice – Crime and Courts Act 2013, 11 February 2014, at para. 2.8.2(i).

12 *Serious Fraud Office v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc* (U20170036). Rolls-Royce first came to the attention of the SFO in early 2012, when a whistleblower raised concerns about Rolls-Royce's business in China and Indonesia. After a lengthy investigation, Rolls-Royce accepted responsibility for criminal offending over 24 years, across seven different countries. Ultimately, Rolls-Royce was granted a DPA, and paid approximately £800 million in financial penalties to authorities in the UK, US and Brazil.

13 See e.g. memorandum dated 5 July 2007 from Paul J. McNulty re Principles of Federal Prosecution of Business Organizations available at https://www.justice.gov/sites/default/files/dag/legacy/2007/07/05/ mcnulty_memo.pdf

14 In March 2017, DOJ announced that the Pilot Program, which was originally intended to terminate on 5 April 2017, will remain in place while DOJ continues to evaluate the program.

tary self-disclosure of wrongdoing' the disclosure will have to be made 'prior to an imminent threat of disclosure or government investigations' and 'within a reasonably prompt time after becoming aware of the offense'. Moreover, the company will have to disclose 'all relevant facts known to it, including all relevant facts about the individuals involved in any FCPA violation.'[15] Voluntarily producing documents to an investigating authority, without the need for a formal request, helps demonstrate a truly proactive approach by the company. There may also be more room to negotiate the scope of the voluntary disclosure than where a company receives a formal request.

Timing is important, both for a potential DPA and in relation to anti-cartel regimes, which often provide an amnesty only to the first discloser.[16]

As has been noted above, the FCA's standard practice is to rely on its statutory powers to require the production of documents. While there is merit in adopting this policy, and it does avoid the risks to companies of voluntarily disclosing documents to the FCA set out below, nothing prevents the FCA from seeking voluntary production. Principle 11 of the FCA's Principles for Businesses states that: 'A firm must deal with its regulators in an open and co-operative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice.' A materially identical provision is included in the Prudential Regulation Authority's (PRA) Rulebook as Fundamental Rule 7. While this chapter focuses on the approach of the FCA, it is worth remembering that the PRA has similar enforcement powers (and is using them with increasing frequency). Both regulators interpret these obligations to proactively bring matters to their attention widely, and are prepared to take enforcement action against firms and individuals for failures to discharge these obligations (even in the absence of other underlying failings). Prudential Group (fined £30 million for failing to inform the FSA of its proposed acquisition of AIA until after it had been leaked to the media), Goldman Sachs (fined £17.5 million for not disclosing an SEC investigation into its staff and members of The Goldman Sachs Group), and the Co-operative Bank (issued a final notice for failing to notify the PRA without delay of two intended personnel changes in senior positions) are recent examples. This places regulated firms in a different position from other corporates: it reduces the scope for the decision whether to self-report or not.

Principle 11 is mainly intended as a supervision tool and sets out a broad duty of co-operation that the FCA often relies on to oblige the production of documents prior to formal investigations being commenced (sometimes, but

---

See remarks prepared for delivery by Kenneth A. Blanco, Acting Assistant Attorney Gen. Kenneth A. Blanco Speaks at the American Bar Association National Institute on White Collar Crime (10 March 2017), available at https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-american-bar-associationnational.

15 US Department of Justice, The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance, 5 April 2016, at p. 4.

16 See e.g. European Commission Notice on Immunity from Fines and Reduction of Fines in Cartel Cases, Official Journal C 298, 8 December 2006, p. 17.

not always, for the purpose of deciding whether an investigation should be commenced and, if so, in respect of which firms and individuals). The FCA's view of what is meant by being open and co-operative within Principle 11 is set out in the FCA Handbook, in the 'Supervision' section (referred to as SUP). SUP 2.3 provides that 'open and co-operative' includes a regulated entity making itself readily available for meetings with the FCA, giving the FCA reasonable access to records, producing documents as requested, and answering questions truthfully, fully and promptly. Where a formal investigation has been commenced, the FCA would not seek to rely on Principle 11 as a substitute for its other statutory powers that compel production. While it would be a clear breach of Principle 11 to fail to comply with a statutory request for the production of documents, a failure to comply with a voluntary request for the production of documents would not, of itself, result in disciplinary proceedings. The Enforcement Guide does state, in the context of co-operation, that:

> *The FCA will not bring disciplinary proceedings against a person for failing to be open and co-operative with the FCA simply because, during an investigation, they choose not to attend or answer questions at a purely voluntary interview. However, there may be circumstances in which an adverse inference may be drawn from the reluctance of a person (whether or not they are a firm or individual) to participate in a voluntary interview. If a person provides the FCA with misleading or untrue information, the FCA may consider taking action against them.*[17]

The Enforcement Guide further provides that if a person does not comply with a requirement imposed by the exercise of statutory powers, he or she may be held to be in contempt of court. The FCA may also choose to bring proceedings for breach of Principle 11.[18] Therefore, while there is no guidance indicating that a failure to produce documents voluntarily (as opposed to attending a voluntary interview) would result in an adverse inference being drawn, a decision by a company not to produce documents voluntarily in any particular case should not be made without careful forethought and proper advice on the potential consequences.

As this suggests, the Enforcement Guide recognises the importance of an open and co-operative relationship with the firms it regulates to the effective regulation of the UK financial system. When deciding whether to exercise its enforcement powers, the FCA considers, among a number of factors, the level of co-operation demonstrated by a firm. When weighing the level of co-operation, the FCA considers whether the firm has been open and communicative with it.

Voluntarily disclosing documents carries a risk that the authority may not give any meaningful credit and may nonetheless decide to prosecute or expand an investigation already under way. Therefore, the company should weigh the

17 See Enforcement Guide, at para. 4.7.3.

18 Ibid. at para. 4.7.4.

likelihood of the authority being able to serve a formal request for disclosure in the relevant jurisdiction.

In some instances, a formal notice for disclosure will be preferred: for example, where a company has obligations of confidentiality, preventing voluntary disclosure. The most common examples being lawyers and financial institutions who could both face an action for breach of confidence for supplying documents or information without a formal regulatory request. In some self-reporting circumstances, it may be appropriate for a company to seek such a notice from the relevant authority to ensure that it does not open itself up to civil action. The notice should be narrowly drawn, in consultation with the regulator, and should not affect the company's co-operation credit. Likewise, in some situations, the company may prefer to ask to be provided with a formal document request to demonstrate that they have been compelled to produce the documents to the authorities and have not done so voluntarily.

See Section 11.2.4.6, and Chapters 35 and 36 on privilege

Production of information to multiple authorities 11.2.3

The increasingly complex and multi-jurisdictional nature of investigations means that a company may face requests for formal disclosure from more than one authority. This could be authorities with different mandates within the same jurisdiction, or authorities with similar mandates from different jurisdictions. In either case, multi-authority investigations demand holistic strategies and systems to allow a company to keep track of evidence disclosed to (or seized by) different authorities. A company may also want to consider if there is any strategic advantage to disclosing to one authority before another. However, recent large-scale global investigations into the manipulation of LIBOR and foreign exchange rates demonstrate the ever increasing levels of intra- and international co-operation between regulators.[19] Practical steps a company can take when faced with multiple requests for formal disclosure include:

- early engagement with each authority, to communicate expectations and practical difficulties of responding to multiple requests;
- identifying and prioritising information that is commonly responsive to the requests rather than focusing on responding to each individual request in isolation;
- maintaining clear production schedules; and
- ensuring a system for Bates numbering[20] for each authority.

19 In 2015, Deutsche Bank AG entered into a DPA with the DOJ and settlements with the US Commodity Futures Trading Commission, the Department of Financial Services and the FCA, in connection with its role in manipulating LIBOR rates. DB Group, a subsidiary of Deutsche Bank, also pleaded guilty to wire fraud for its role. Together, Deutsche Bank and its subsidiary agreed to pay over US$2 billion in penalties to US authorities and US$344 million to the FCA – then the second-largest fine in the FCA's history.

20 Bates numbering is a method of indexing legal documents for easy identification and retrieval.

11.2.4 Documents and data outside the jurisdiction

11.2.4.1 Voluntary production

In cross-border fraud or corruption cases, not all of a company's documents will be located or even accessible in the same jurisdiction as the investigating authority. A company should consider what documents are stored overseas, and which of these it should provide to investigators. A company in receipt of a formal production notice will need to assess whether the notice extends to documents outside the jurisdiction, and, if so, the extent to which the company has 'custody or control' over documents held by subsidiaries or overseas branches.[21] The board of a parent company will not necessarily control the management of a subsidiary.[22] Where production is voluntary, a company may take a more holistic view of the investigation and production (subject to local law restrictions). The extent to which it may want to voluntarily disclose information may depend on the ability of the investigating authority to obtain that information itself. However, given the increasing co-operation between authorities on the international stage, careful voluntary production of material is likely to be preferable, and vital if the company seeks co-operation credit.

11.2.4.2 Mutual legal assistance

In the United Kingdom, sections 7–9 of the Crime (International Co-operation) Act 2003 (CICA) govern requests to obtain evidence from abroad in relation to a prosecution or investigation taking place in the United Kingdom, shaping the mutual legal assistance (MLA) powers of UK authorities. Under CICA, an MLA request can only be made if it appears to the investigating authority that an offence has been committed or there are reasonable grounds for suspecting that an offence has been committed, and either proceedings in respect of that offence have been instituted or the offence is being investigated.[23] The request must relate to the obtaining of evidence 'for use in the proceedings or investigation'.[24] But, it could allow an investigating agency to have foreign law enforcement officers launch raids, arrest suspects or conduct interviews on its behalf.[25] If the implementation of an MLA request in the requested state requires a court order, then the court in the requested state is likely to apply the relevant principles in its own jurisdiction to satisfy itself that the requested order is justified.

Note that among the vast majority of EU Member States, European investigation orders (EIOs) now allow streamlined access to evidence and information in

21 Production notices seeking documents held outside the jurisdiction of the investigating authority are complicated. For example, the authors take the view that a request made under s.165 of FSMA captures documents in a company's custody or control outside the United Kingdom, while a request under s.2 of the Criminal Justice Act does not.

22 For the United Kingdom see *Lonrho v. Shell Petroleum* [1980] 1 WLR 627.

23 Crime (International Co-operation) Act 2003, s.7(5).

24 Ibid., s.7(2).

25 See e.g. Reuters, 'Monaco raids Unaoil offices over global oil corruption probe', available at http://uk.reuters.com/article/uk-oil-companies-corruption-idUKKCN0WY3KM.

criminal investigations. EIOs work on the basis of mutual recognition, and judicial authorities can use them to request assistance with 'any investigative measure' (although the EIO itself will identify a number of investigative activities that it does not permit). More specifically, the EIO:

- replaces the previous fragmented legal framework for obtaining evidence within Europe by providing a single instrument;
- imposes a strict 30-day deadline for the Member State to accept the request, and 90 days to comply;
- limits the reasons for which the Member State can refuse the request;
- introduces a standard form; and
- prioritises the necessity and proportionality of the measure as part of the rights of the defence.

EIOs were created by EU Directive 2014/41/EU, which came into force in the United Kingdom on 31 July 2017 (transposed through the Criminal Justice (European Investigation Order) Regulations 2017). The United Kingdom has opted into the EIO regime even though it has chosen to exit the European Union.

The MLA process can be cumbersome, but is a very real threat in the event a company does not co-operate. A company should also not overlook the significant scope for informal direct investigator-to-investigator co-operation. Agencies such as Interpol have dedicated programmes to share information between, and support investigations by, investigating agencies in different countries. Communications between the SFO and DOJ are frequent. The FCA, specifically, has a broad discretion to assist foreign regulators. This discretion is set out in section 169 of FSMA. The statutory power is supplemented by relevant FCA policy. Subsection 169(4) sets out the considerations in the FCA's decision as to whether to assist a foreign regulator. It provides:

> *(4) In deciding whether or not to exercise its investigative power, the regulator may take into account in particular:*
>
> *(a) whether in the country or territory of the overseas regulator concerned, corresponding assistance would be given to a United Kingdom regulatory authority;*
>
> *(b) whether the case concerns the breach of a law, or other requirement, which has no close parallel in the United Kingdom or involves the assertion of a jurisdiction not recognised by the United Kingdom;*
>
> *(c) the seriousness of the case and its importance to persons in the United Kingdom;*
>
> *(d) whether it is otherwise appropriate in the public interest to give the assistance sought.*

In an early decision on this section, *Financial Services Authority v. Amro International*,[26] the Court of Appeal held that there was nothing in section 169 that required the FCA's predecessor body to satisfy itself of the correctness of what it was being asked to investigate or gather by way of information. At the SEC's behest, the FCA could seek any document that it reasonably considered relevant to the investigation the SEC was conducting. The Court of Appeal made clear that the only requirements the FCA must meet were contained in the statute. The Court of Appeal also noted that in exercising these powers, the stricter rules attaching to the drafting of a subpoena did not apply and the description of the documents sought would be acceptable provided the recipient could identify the documents he or she was required to produce.

In addition to the FCA's statutory powers, a number of memoranda of understanding are in place between UK regulators and their overseas counterparts (most notably the SEC and other US regulators) concerning co-operation and information sharing. Recent years have seen significant co-operation between the SEC and the FCA and its cognate agencies.

See Section 11.2.3

Similarly, the United States has entered into mutual legal assistance treaties (MLATs) with various countries, which can be used for the sharing of information and taking of evidence abroad.[27] Some US authorities also have memoranda of understanding in place with sister agencies outside the United States, which can allow for inter-agency sharing of documents.

11.2.4.3 Data protection

Responding to an investigation (and conducting an internal investigation) will require data about individuals to be processed. Such an exercise will engage a number of data protection considerations.[28] A company cannot assume that complying with the data protection requirements in the investigated jurisdiction will mean compliance with overseas data protection laws. European jurisdictions such as France and Germany, for example, have demanding standards for informed consent to a given process. Data protection laws may also prevent the transfer of personal information outside the country of origin: under the UK's Data Protection Act 1998, a company cannot transfer data to countries outside the European Economic Area unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data. In Europe, the European Union's General Data Protection Regulation (GDPR)

26 *Financial Services Authority v. Amro International* [2010] EWCA Civ 123.

27 www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

28 The United States does not have a comprehensive, federal data protection law. There are, however, numerous state and federal laws that govern the treatment of personal data. At the federal level, there are protections for, among other things, data collected from children, from financial institutions and that includes medical information. See, e.g., Federal Trade Commission Act, 15 U.S.C. §§ 41-58; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506; Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 U.S.C. §§ 6801-6827; Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1301 et. seq (and the rules and regulations promulgated thereunder); Fair Credit Reporting Act, 15 U.S.C. § 1681.

is scheduled to come into force on 25 May 2018. Whatever the implications of Brexit for the United Kingdom, the GDPR applies to data controllers and processers outside the EU who offer goods and services to EU consumers. The GDPR introduces a limited derogation to its principles based on 'legitimate interests', which could cover transfers to foreign regulators, but does require prior notification to the relevant data protection authority. However, as a consequence of the Sapin II law, a new body, France's National Anti-Corruption Agency now has specific responsibility for the enforcement of the Blocking Statute, signalling that the French authorities are looking to actively enforce this legislation.

Blocking statutes 11.2.4.4

Blocking statutes prevent the disclosure of certain documents for the purpose of legal proceedings in a foreign jurisdiction, except pursuant to procedures set out in an international treaty or agreement. Article 1bis of the French Blocking Statute provides:

> *[I]t is prohibited for any person to request, to investigate or to communicate in writing, orally or by any other means, documents or information relating to economic, commercial, industrial, financial or technical matters leading to the establishment of proof with a view to foreign administrative or judicial proceedings or as a part of such proceedings.*

There has historically been very little enforcement of the French Blocking Statute – with some companies choosing to ignore it completely. However, as a consequence of the Sapin II law, a new French national anti-corruption agency will be given specific responsibility for the enforcement of the Blocking Statute, signalling that the French authorities are looking to actively enforce this legislation. Similarly, Article 271 of the Swiss Criminal Code prohibits a person performing an 'official act' on behalf of a foreign authority on Swiss soil. This can block the collection of evidence located in Switzerland intended for use in proceedings outside the country.

A decision to refuse to disclose documents or information due to a blocking statute may not be respected by the requesting authority[29] and could affect any co-operation credit available – leaving the company between a rock and a hard place. This demands early and detailed dialogue with the relevant authority alongside expert local counsel advice who can educate the regulators about the relevant laws and any potential workarounds for production of information.

Bank secrecy 11.2.4.5

Bank secrecy laws prohibit banking officials from releasing confidential information about a customer to third parties outside of financial institutions, unless

29 For a recent English case dealing with the French blocking statute, see *Secretary of State for Health v. Servier Laboratories*; *National Grid Electricity Transmission v. ABB* [2014] WLR 4383.

compelled by law. Sometimes, such a disclosure is criminalised.[30] A bank under investigation may seek to rely on this secrecy. It should also be cautious not to infringe this secrecy inadvertently in providing information to a regulator. Note, though, that a historic deference to the banking secrecy rules of foreign jurisdictions, premised on comity or respect for the acts of foreign governments, may slowly be eroding. Even Switzerland, in recent times, has stripped away a number of its many layers of secrecy through international agreements,[31] and, in our experience, has become, in practice, more willing to co-operate with requests for information.

11.2.4.6 State secrets

Sending data outside a jurisdiction may be contrary to state secrecy laws. Some jurisdictions, such as China, have wide definitions of what amounts to a state secret. The Law of the People's Republic of China on Guarding State Secrets, at Article 8, defines state secrets to include 'secrets in national economic and social development' and 'secrets concerning science and technology'. Similarly, Kazakhstan treats some geological data as a state secret. The consequences of violation can be serious. Article 111 of the Chinese Criminal Law makes violating state secrets a capital crime. In countries such as China, where many companies are state-owned, this is not straightforward. Again, locating expert local counsel is a must.

State secrecy laws may also restrict certain categories of documents to authorised eyes only. This is particularly pertinent for defence companies. Withholding production of such documents will require careful negotiation. Remember that the investigating agency is likely to have authorised persons of its own, who can review the documents. Finding a practical way for these to be produced by external lawyers (where prior authorisation is unlikely) will likely be more difficult and undoubtedly will increase the time it will take to respond to a request for documents and may require the review of documents 'in country' instead of producing the documents to the US authorities. Another potential workaround is production of information through MLATs and MOUs that allow a company to first produce documents to a local authority and thereby comply with the relevant regulations.

11.2.4.7 Whose rules of privilege apply?

It may not be clear whose rules of privilege apply when a company discloses in one jurisdiction documents created in another. English courts will generally apply English law to the question: theoretically, an unprivileged document in its country of origin could be privileged in England and *vice versa*. In the United States, there is no general rule, although government agencies will generally apply privilege

30 See most famously Article 47 of the Swiss Federal Act on Banks and Savings Banks (1934).

31 See e.g. Switzerland's entrance, in October 2013, to the Multilateral Convention on Mutual Administrative Assistance on Tax Matters, and agreement to increase transparency and exchange financial information with approximately 60 other countries.

principles broadly, although subject to certain procedural requirements, such as the production of privilege logs.

Companies should also be aware that some countries do not have developed principles of legal privilege and special care is required in creating or sending otherwise-privileged documents to such jurisdictions. Likewise, in some jurisdictions privilege does not extend to communications with in-house counsel and the role of internal counsel may be held by someone who is not an attorney, and therefore privilege may not be recognised in connection with their communications.

Further complications come when dealing with international regulatory bodies. In *Akzo Nobel*, for example, the European Court of Justice held that the law of the European Union superseded that of the relevant national jurisdictions; therefore, in competition cases internal counsel's advice will not be privileged – nor will that of external legal advisers who are not EU-qualified lawyers.[32]

Documents obtained through dawn raids, arrest and search 11.3

During a raid (or execution of a search warrant) on corporate premises, it is important to seek to obtain and understand the terms of the warrant. Check simple facts such as the premises' address, date and relevant powers and authorisations. If appropriate, a company may challenge the scope of the warrant (if it is unduly wide or based on erroneous facts or information). Importantly, the company and its advisers should ensure during the raid that documents outside the terms of the warrant are not seized (unless taken under relevant search and sift powers,[33] or as can be justified under ancillary legislation[34]) and take care both during the raid and afterwards to protect legally privileged materials. In the United States, it is nearly impossible to challenge the scope of a warrant that calls for the immediate search of a specific location. More likely, a company would have to seek to suppress evidence obtained pursuant to a warrant in a later proceeding. There may, however, be opportunities to challenge the scope of a warrant seeking electronically stored information before the data is actually collected and produced.[35] As an example, where a company is asked to execute a warrant on behalf of the government, such as when a service provider is asked to collect electronic information of a third party, there may be additional opportunities for a company to challenge the scope of a subpoena. Recently, Microsoft was successful in challenging

32 *Akzo Nobel Chemicals v. European Commission* (Case C-550/07, European Court of Justice, 14 September 2010). Here, the Court held that internal company communications with in-house lawyers subject to a European Commission investigation were not covered by legal professional privilege, as, for the purposes of such an investigation, an in-house lawyer was not sufficiently independent.

33 For the United Kingdom, see s.50 of the Criminal Justice and Police Act 2001.

34 See s.19(5) of the Police and Criminal Evidence Act 1984.

35 See *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, F893 F.3d 197 (2d Cir. 2016) (finding that the government could not compel Microsoft to collect data held outside of the United States that was requested in a warrant issued pursuant to the Stored Communications Act).

the scope of a warrant issued pursuant to the Stored Communications Act.[36] Specifically, Microsoft was served with a warrant seeking data held on servers in Ireland. It challenged the collection of the relevant information, arguing that it was not permitted to make the collection based on data privacy laws in the jurisdiction where the data was held. A US Court of Appeals agreed, finding that the Stored Communications Act (the law pursuant to which the warrant was issued) could not be used to compel collection of data outside the United States. There has been significant disagreement with this ruling, even within the court that affirmed the initial decision,[37] and courts have required service providers including Google and Yahoo! to respond to warrants requiring the production of data held outside the United States.[38]

It is likely that the vast majority of documents obtained during a search will be electronic. It is important to agree to a process with the authorities for dealing with any electronic media that is privileged. In the United Kingdom, most investigative agencies have developed sophisticated procedures in this area. The SFO's policy and system for dealing with material covered by legal professional privilege (LPP) is explained in its Operational Handbook:[39]

> *When the SFO requires the production of material, or seizes material pursuant to its statutory powers, all material which is potentially protected by LPP must be treated with great care to:*
>
> - *Minimise the risk that LPP material is seen or seized by an SFO investigator or a lawyer involved in the investigation.*

36 Id.

37 See *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 855 F.3d 53 (2d Cir. 2017), 2017 WL 362765 (2d Cir. 24 January 2017) (denying request for rehearing *en banc* but incorporating dissenting opinions explaining disagreement with original finding that Microsoft could not be compelled to produce data held in Ireland).

38 See e.g. *In re Search Warrant No. 16–960–M–01 to Google*, 2017 WL 471564 (E.D. Pa. 3 Feb. 2017) (ordering Google to comply with search warrants seeking data held on servers outside of the United States); *In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo*, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. 21 February 2017) (determining that a court can compel a service provider within its jurisdiction to disclose data within its control regardless of where the data is located); *Matter of Search of Content that is Stored at Premises Controlled by Google*, 2017 WL 1487625 (N.D. Cal. 25 April 2017) (compelling producing of data held on servers outside of the United States but distinguishing situation from Microsoft case because Google's storage of data outside the United States was not related to the location of the account holder).

39 See the unsuccessful challenge to this procedure in *R (McKenzie) v. Director of the Serious Fraud Office* [2016] EWHC 102 in which the essential question was whether, as a matter of law, the process for isolating files that may contain LPP material into an electronic folder for review by an independent lawyer must itself be carried out by individuals who are independent of the seizing body. The court held that the procedure set out in the SFO's Handbook for isolating material potentially subject to LPP, for the purpose of making it available to an independent lawyer for review, was lawful.

- *Ensure that any LPP material which is seized is properly isolated and promptly returned to the owner without having been seen by an SFO investigator or a lawyer involved in the investigation.*
- *Ensure that any dispute relating to LPP is resolved in advance of the material being seen by an SFO investigator or a lawyer involved in the investigation.*
- *Ensure that where an SFO investigator or a lawyer involved in the investigation inadvertently sees LPP material, measures are in place to ensure that the investigation and any subsequent prosecution is not adversely affected as a result. Care must always be taken that LPP material is not viewed by the SFO staff involved in the investigation.* [Original emphasis.]

The Operational Handbook then sets out a procedure for dealing specifically with electronic material that may be privileged. Under this procedure, the SFO will first notify the company's lawyers if it believes that IT assets it has seized might contain privileged material (in practice, it is prudent for the company's lawyers to advise the SFO of the potential existence of privileged material at an early stage). A list of search terms should be agreed (including names of lawyers, relevant firms, etc.) to enable the identification and isolation of the material for review by independent counsel. Independent counsel will review the material using search software and return only non-privileged material to the SFO investigative team to examine. It is normally possible to have productive discussions with investigators to determine the relevant search terms that might identify privileged material. It is then possible to make representations on the client's behalf to independent counsel about the extent of privilege. This procedure updates and works alongside the well-established 'blue-bagging' approach used for hard-copy materials that may be privileged, by which authorities will send seized documents that may be potentially privileged, sealed in an opaque bag, to the custody of an independent legal adviser (usually a barrister) for review.

The DOJ has utilised three different procedures for reviewing potentially privileged information, each of which requires a 'neutral' third-party to first review potentially privileged data.[40] In certain instances the court may review the data on its own. A court may also appoint a 'special master' to handle the review of privileged information. In other instances, a team of individuals referred to as a 'taint team' may be used to review the files. When a taint team is used, an ethical wall will be placed between the individuals who review the documents and those who are actually participating in the investigation. Importantly, courts have had differing reactions to the use of taint teams and may not always conclude that the procedures implemented to screen materials were sufficient.

40 See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

11.4 Disclosure of results of internal investigation

In most instances, a company will have to make expansive disclosures regarding its internal investigations to get full co-operation credit. The DOJ has issued guidance through the Yates Memorandum[41] and the FCPA Pilot Program[42] that explicitly states that companies will have to self-report on both the results of internal investigations and on individual misconduct to receive any co-operation credit. Whether such thorough disclosures are in the best interest of the company is something that will need to be determined in a timely manner.

11.4.1 Self-reporting of misconduct not yet known to regulators

A company's decision as to whether to self-report is often complicated. There may be opportunities for a company to internally address misconduct without it coming to light. However, it can be very difficult for a company to keep its misdeeds from being disclosed to the relevant authorities. Whistleblower rewards provide incentives for employees to report misconduct. Federal statute provides protections for whistleblowers,[43] and the SEC has recently imposed financial penalties on financial institutions that attempt to prohibit employees from seeking those bounties.[44] Disgruntled employees can report corporate misconduct as retaliation, to attempt to prevent prosecution of themselves or simply because they do not feel that the corporate is handling the issue appropriately via its internal process. In the United Kingdom, broadly speaking, those working in the field of financial services are subject to suspicious activity reporting obligations. This means that banks, accountants and transactional lawyers must make reports to the authorities of suspicions of money laundering (including acquiring assets which may be tainted by fraud or corruption). A failure to make a report is a criminal offence – as is tipping off the subject of the report (which in some instances may be the individual's own client). Investigative journalism and NGOs also continue to be important sources of information for regulators – as the recent 'Panama Papers' scandal has shown.[45]

A failure to self-report misconduct before it becomes otherwise known to the authorities can have a significant impact on the resolution of the corporate investigation. The US Attorneys' Manual (USAM) (which governs the conduct

41 Memorandum dated 9 September 2015 from Sally Quillian Yates re Individual Accountability for Corporate Wrongdoing available at https://www.justice.gov/dag/file/769036/download.

42 Memorandum dated 5 April 2016 re The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance available at https://www.justice.gov/opa/file/838386/download.

43 See Section 922(h) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 15 U.S.C.A. § 78u-6(h)(1)(A) (2010).

44 See https://www.sec.gov/news/pressrelease/2017-14.html (announcing penalty imposed on Blackrock Inc. based on its inclusion of language in separation agreements requiring former employees to waive any incentives they might be entitled to for reporting the company's misconduct); https://www.sec.gov/news/pressrelease/2017-24.html (announcing penalty imposed on HomeStreet Inc. for improper accounting and steps taken to impede whistleblowers).

45 The Panama Papers are available through the ICIJ's (The International Consortium of Investigative Journalists) dedicated website: https://panamapapers.icij.org/.

of assistant US Attorneys during the course of civil and criminal investigations, including FCPA investigations) has been revised to provide that:[46]

> *Even in the absence of a formal program, prosecutors may consider a corporation's timely and voluntary disclosure, both as an independent factor and in evaluating the company's overall cooperation and the adequacy of the corporation's compliance program and its management's commitment to the compliance program. However, prosecution may be appropriate notwithstanding a corporation's voluntary disclosure. Such a determination should be based on a consideration of all the factors set forth in these Principles.*

As we have already noted, under the FCPA Pilot Program, 'for a company to receive credit for voluntary self-disclosure of wrongdoing', the disclosure will have to be made 'prior to an imminent threat of disclosure or government investigations' and 'within a reasonably prompt time after becoming aware of the offense'. Moreover, the company will have to disclose 'all relevant facts known to it, including all relevant facts about the individuals involved in any FCPA violation.'

The Deferred Prosecution Agreements Code of Practice (DPA Code) issued by the SFO and CPS[47] indicates that, to be eligible for a DPA, a company will likely have to report voluntarily any misconduct within a reasonable time of becoming aware of it – and prior to it becoming known to the authorities. In fact, in both of the previous DPA cases,[48] the companies self-reported their misconduct to the SFO in circumstances where the SFO had no prior knowledge of the misconduct and, in all likelihood, would not have learnt about the misconduct if the company had not self-reported.

But, in the recent *Rolls-Royce* case, the company did not self-report to the SFO the conduct that led to the SFO's investigation. Instead, the SFO became aware of the need for an investigation through internet postings by a whistleblower. The fact that Rolls-Royce did not self-report weighed against the SFO offering a DPA; yet, Rolls-Royce chose to co-operate fully with the investigation after the SFO approached them, and undertook its own internal investigation (in close consultation with the SFO). In total, Rolls-Royce collected over 30 million documents and subjected them to electronic document review as part of this investigation. One of the main features of Rolls-Royce's co-operation was that it provided all materials requested by the SFO voluntarily, without the SFO having to compel it to provide information. Rolls-Royce also chose not to perform any legal professional privilege review over the documents (instead allowing independent counsel resolve issues of privilege), and worked with the SFO as the SFO used sophisticated search techniques to interrogate the data. This led to the SFO uncovering information that may not have otherwise come to its attention. Ultimately, SFO

46 USAM 9-28.900 (internal citations omitted).

47 Para. 2.8.2(i) DPA Code.

48 *SFO v. Standard Bank plc* (U20150854) and *SFO v. XYZ Ltd* (U20150856).

counsel described the extent of Rolls-Royce's co-operation with the investigation as 'extraordinary'.

While the decision to provide documents voluntarily to the SFO was one of a number of measures taken by Rolls-Royce to demonstrate its co-operation with the investigation, this decision was of fundamental importance to the court when deciding to approve the DPA. Rolls-Royce's voluntary disclosure of investigation documents therefore mitigated its failure to voluntarily disclose misconduct.

11.4.2 Production of reports of investigation

To obtain co-operation credit, prosecuting and government agencies require that companies provide the complete factual findings of an internal investigation, including relevant source documents. The USAM recognises 'the sort of cooperation that is most valuable to resolving allegations of misconduct by a corporation and its officers, directors, employees, or agents is disclosure of the relevant facts concerning such misconduct.'[49] The Yates Memorandum notes that:

> *[T]o be eligible for <u>any</u> credit for cooperation, the company must identify all individuals involved in or responsible for the misconduct at issue, regardless of their positions, status or seniority, and provide to the Department all facts relating to that misconduct.* [Emphasis added.]

The FCPA Pilot Program requires that to receive credit for voluntary self-disclosure, a company must disclose all relevant facts. Similarly, the DPA Code provides that co-operation will include 'providing a report in respect of any internal investigation including source documents.'[50]

Careful consideration should be given to the manner of disclosure of information. In the United States, the consideration for credit is that the relevant facts are disclosed. The format of the disclosure is irrelevant. The USAM makes clear that a company does not have to waive privilege to receive co-operation credit.[51] If a company chooses not to waive relevant privileges, it is unlikely to be able to share the investigative reports prepared by counsel conducting the investigation. Instead, it will have to carefully craft presentations that disclose only non-privileged facts. Preparation of such reports can be time-consuming and costly. Further, in preparing any written presentation materials the company will have to ensure that neither the mental impressions nor advice of counsel are included. Because there can be no claim that the materials are privileged, a company should also expect that they will have to produce presentation materials in any related civil litigation.

In the United Kingdom, there is currently much debate over the production of the first accounts of witnesses, which may have been taken by investigating attorneys. The SFO's preference is that these are taken so that legal privilege does not apply. It also indicates that it does not consider all privilege claims over interview

49 See USAM 9-28.720 ('Cooperation: Disclosing the Relevant Facts').

50 Para. 2.8.2(i) DPA Code.

51 See USAM 9-28.720.

materials to be made out under English law and is actively challenging such assertions. Where a valid claim for privilege exists, co-operation credit will be given for the disclosure of interview memoranda. A failure to disclose will be considered co-operation neutral. As Alun Milford, SFO General Counsel, has recently said, '[i]f 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.'[52] In two of the UK cases in which the court has approved DPAs, the company made oral disclosure only of the content of witness interviews.[53] However, Rolls-Royce chose to provide the interview memoranda to the SFO – even though it considered the memoranda to be privileged – on the basis of a limited waiver of privilege. This was another way Rolls-Royce used the voluntary disclosure of documents to counterbalance its failure to voluntarily disclose the misconduct. Other materials voluntarily provided to the SFO by Rolls-Royce included regular reports on the findings of the internal investigations; unfiltered access to the 'digital repositories or email containers' for over 100 past and present employees; general access to hard copy documents at Rolls-Royce; and key documents identified by the internal investigations. Finally, Rolls-Royce held off interviewing potential witnesses until the SFO had the chance to do so. How a company makes its employees available to investigating authorities is important, and this chapter will now turn to this issue.

Identification of witnesses to authorities 11.4.3

In connection with its initial assessments of whether to co-operate with authorities, companies will have to consider the implications of disclosing information about key employees. As noted above, US and UK authorities have indicated that co-operation will require disclosure of facts relevant to the misconduct of individual employees.

In the United States, authorities have recently made clear that obtaining facts relevant to individual prosecutions is a top priority. In the Yates Memorandum, the DOJ stated that '[o]ne of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing.' It went on to identify and discuss in detail six key steps to strengthen the DOJ's pursuit of individual wrongdoing including:

52 Alun Milford, SFO General Counsel, 'Speech to compliance professionals' (Speech given to the European Compliance and Ethics Institute, Prague, 29 March 2016).

53 See e.g. *SFO v. XYZ* (Preliminary Judgment) Crown Court, Southwark, U20150856 (20 April 2016): '[C]o-operation includes identifying relevant witnesses, disclosing their accounts and the documents shown to them: see para. 2.8.2(i) of the DPA Code of Practice. Where practicable it will involve making witnesses available for interview when requested. In that regard, XYZ provided oral summaries of first accounts of interviewees, facilitated the interview of current employees, and provided timely and complete responses to requests for information and material, save for those subject to a proper claim of legal professional privilege.'

> *1. To be eligible for <u>any</u> co-operation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct.'* [Original emphasis.]
>
> . . .
>
> *2. Both criminal and civil corporate investigations should focus on individuals from the inception of the investigation.*

These principles have been incorporated into the USAM and into the FCPA Pilot Program. Additionally, the 'unequivocal co-operation' necessary to be eligible for a DPA in the United Kingdom includes identifying relevant witnesses, disclosing their accounts of the alleged misconduct and any documents shown to them and, where practicable, making those witnesses available for interviews by investigators[54] – together with ongoing co-operation with the authorities.

Once the individuals have been identified to the government or prosecuting authorities it may be difficult, if not impossible, for those individuals to continue working for the company. A company may feel pressure to terminate the employee or place that individual on leave, which could have a significant impact on the operations of a business unit. Even if the company does not terminate an employee under investigation, targets of a government investigation are likely to engage their own counsel who may advise the employee to stop co-operating with its employer – leading to a 'walk or talk' decision. Depending on the nature of any employment agreement, a company may have to advance the individual the fees and costs associated with individual representation. Also, since 2004, the United Kingdom has imposed an extensive Code of Practice for Disciplinary and Grievance Procedures on employers, which sets out standards of procedural fairness that a UK employer should comply with if it takes action that will detrimentally affect an employee's employment.[55]

See Chapters 13 and 14 on employee rights

11.5 Privilege considerations

In the United States, certain portions of internal investigations are protected by the attorney–client privilege and the work-product doctrine, and courts routinely uphold those privileges.[56] This can be true even where the purpose of an investigation is to ensure regulatory compliance, or where non-lawyers are involved in key parts of the investigation.[57]

Generally, the attorney–client privilege entitles a party to withhold from production (1) communications, (2) with an attorney, his or her subordinate or

54 DPA Code, para. 2.8.2(i).

55 ACAS 'Code of Practice on Disciplinary and Grievance Procedures' (2015) available at www.acas.org.uk/media/pdf/f/m/Acas-Code-of-Practice-1-on-disciplinary-and-grievance-procedures.pdf.

56 See *In re Kellogg Brown & Root, Inc.,* 756 F.3d 754 (D.C. Cir. 2014).

57 Id. at 760 ('In the context of an organization's internal investigation, if one of the significant purposes of the internal investigation was to obtain or provide legal advice, the privilege will apply. That is true regardless of whether an internal investigation was conducted pursuant to a company compliance programme required by statute or regulation, or was otherwise conducted pursuant to company policy.') (citation omitted).

agent, (3) made in confidence, (4) for the primary purpose of securing an opinion of law, legal services or assistance in a legal proceeding. It applies to corporations as well as individuals, and therefore protects communications between corporate employees and a corporation's in-house and outside legal counsel on matters within the scope of the employees' corporate responsibilities. Communications between non-legal corporate employees can also be privileged where an attorney neither authors nor receives the communication, if the communication contains or refers to previously transmitted legal advice or identifies specific legal advice that the non-attorneys will seek from attorneys in the near future. Additionally, the work-product doctrine protects documents and tangible things, otherwise discoverable, prepared in anticipation of litigation and in connection with a threatened or pending government investigation. The doctrine can apply to documents prepared by both attorneys and non-attorneys. Attorney notes, research, and compilations of background materials, memoranda, investigative reports, witness statements; and materials prepared by non-legal personnel such as investigators are examples of the types of documents that may be protected. Work-product containing an attorney's mental impressions is referred to as 'opinion' work-product and is afforded greater protection than other 'ordinary' work-product.

In the United Kingdom, privilege attaches to (1) confidential communications between a lawyer and his or her client for the purpose of seeking and receiving legal advice in a relevant legal context, including factual reporting (legal professional privilege), and (2) confidential communications between a lawyer and his or her client and/or a third party or between a client and a third party, provided that such communications have been created for the dominant purpose of obtaining legal advice, evidence or information in preparation for actual litigation, or litigation that is 'reasonably in prospect' (litigation privilege). English case law has long called into question the availability of litigation privilege for documents created during a regulatory investigation. In *Rawlinson and Hunter Trustees SA v. Akers*,[58] the Court of Appeal upheld a High Court decision that:

> *The mere fact that a document is produced for the purpose of obtaining information or advice in connection with pending or contemplated litigation, or of conducting or aiding in the conduct of such litigation, is not sufficient to found a claim for litigation privilege. It is only if such purpose is one which can properly be characterised as the dominant purpose that such claim for litigation privilege can properly be sustained.*

In the recent decision of *Property Alliance Group Limited v. The Royal Bank of Scotland*,[59] the High Court confirmed that the test remained an objective assessment of the dominant purpose of collecting the information. In that case, where one party sought to obtain evidence for litigation, and misled the other parties to

58 [2014] EWCA Civ 136.

59 *Property Alliance Group Limited v. The Royal Bank of Scotland* [2016] 4 WLR 3 at [41]–[42].

a meeting to do so, the Court performed the objective assessment from the misled parties' point of view.

A key consideration is therefore the reason for the creation of the document. The Court of Appeal in *Rawlinson and Hunter Trustees* confirmed that where documents are created for multiple purposes, those purposes will not necessarily be independent of each other. However, the burden is on the party claiming privilege to demonstrate that the purposes are related and that the dominant purpose was for use in the conduct of litigation. This will protect communications with third parties outside the narrowly defined concept of the 'client' under English law. Even though this was not the context of the *Rawlinson and Hunter Trustees* case, some UK white-collar crime experts consider it as authority for the proposition that employee accounts provided during an internal investigation with a view to making a self-report may not be privileged.[60] Whether such a challenge to privilege in employee accounts is successful will depend on the case.

Another key consideration is when litigation in a criminal context is reasonably in prospect. This point was explained in the recent High Court case of *Director of the SFO v. ENRC*.[61] The court held that a company must have uncovered actual evidence of wrongdoing before it could successfully assert that adversarial proceedings were in reasonable contemplation. Andrews J also distinguished between the reasonable contemplation of a criminal investigation and the reasonable contemplation of a prosecution. Documents produced in contemplation of the former only would not be privileged. This decision makes it harder to assert litigation privilege over documents generated in the course of an internal investigation, particularly where a company wishes to instruct lawyers to investigate matters that may suggest criminal wrongdoing, but has not yet uncovered evidence of wrongdoing. Authorities in both the United States and the United Kingdom have made clear that a company does not need to waive any applicable privileges to receive co-operation credit. However, it may be difficult for attorneys to find ways to present all facts discovered during an internal investigation in a manner that does not disclose privileged information.

See Chapter 35 on privilege

In presenting the underlying facts of an internal investigation, a company must be mindful of the inherent risk that such a presentation will be deemed a privilege waiver in any subsequent proceedings. If a disclosure of privileged information to a federal office or agency is deemed intentional, the privilege will be waived in any federal or state proceeding.[62] However, if a disclosure of privileged information is unintentional, it will not create a broad waiver so long as the holder of the privilege took steps to prevent the disclosure and then promptly took reasonable steps to seek return of any inadvertently disclosed information.[63] Accordingly, if

60 See e.g. S Balber, J O'Donnell and E Head, 'Cross-border overview: maximising privilege protection under US and English law' in *The Investigations Review of the Americas 2016* (Global Investigations Review, 2015).

61 *SFO v. ENRC* [2017] EWHC 1017 (Ch).

62 See Fed. R. Evid. 502(a).

63 See Fed. R. Evid. 502(b).

a company decides that it does not intend to waive privilege, it should devise reasonable steps that highlight the company's decision not to waive privilege, including providing written notice of the intention not to produce privileged materials in any letter or other correspondence that accompanies a document production. Courts in England and Wales have held that a company can share the contents of a privileged communication with a regulator or other third party, keeping the privilege intact, so long as this desire is made clear, the disclosure is confidential, and the communication is not proliferated widely.[64]

See Chapters 35 and 36 on privilege

Protecting confidential information 11.6

Companies producing information to the government should take steps to protect the confidentiality of that information. Although information produced in response to a grand jury subpoena must be kept confidential,[65] in the absence of a formal request, documents and testimony provided the DOJ, SEC or other government authority can be shared with others. In many instances, documents under the control of a government agency can be subject to requests made pursuant to the Freedom of Information Act (FOIA).[66] Further, documents typically shielded from disclosure by the FOIA and other regulations are not exempt from production to the United States Congress, which can, in turn, make the information public.

The procedures necessary to shield confidential information from disclosure can be quite complex. Each regulatory body has its own procedures for seeking confidential treatment of information. The SEC, for example, requires that each page of a document containing confidential information be stamped with a specific legend and that a request for confidential treatment go to the individual receiving the documents and the Office of Freedom of Information and Privacy Act Operations.[67] Many states have their own versions of the Freedom of Information Act governing the treatment of information provided to, among others, state attorneys general.[68] Further, while some congressional committees may implement their own procedures for seeking confidential treatment of information, an entity producing documents will have to consider what regulations apply to the information sought and whether the specific regulations prohibit disclosure in response to the request.

In the UK, the High Court confronted these issues in *Standard Life Assurance v. Topland Col*.[69] The SFO had disclosed information it had obtained through its section 2 powers to a Standard Life employee that it wished to interview. The SFO later discontinued the related investigation. Standard Life then used some of this information as part of civil proceedings against Topland. The court noted

64 See *Gotha City v. Sotheby's* [1998] 1 WLR 114 (CA).

65 Fed. R. Crim. Pro. 6(e).

66 5 U.S.C. § 552.

67 17 C.F.R. § 200.83

68 See, e.g., New York Freedom of Information Law, Public Officer's Law §§ 84-90.

69 *Standard Life Assurance Ltd v. Topland Col* (Rev 1) [2011] 1 WLR 2162.

that the SFO was not entitled to disclose any material obtained by it during an investigation except for the purpose of its investigation (which was the original purpose of the disclosure in this case). A person who wished to prevent disclosure of genuinely confidential information, either by the SFO or by a person SFO had disclosed documents to, would need to rely on judicial review proceedings or seek an injunction to prevent a breach of confidence. This suggests that, to avoid relying on these indirect remedies, a company should discuss with the SFO before disclosure how the SFO might control the further dissemination of confidential or sensitive documents. Safeguards may include the SFO returning the documents following a short time, or notifying a disclosing party before the SFO intended to disseminate documents further.

11.7 Concluding remarks

Companies have an incentive to co-operate with a government investigation, especially if co-operation credit does not necessarily require self-reporting of the misconduct. But, self-reporting will assist companies alongside the voluntary provision of relevant materials. The additional advantages of co-operation – control of the investigation process, orderly production of materials and managing press intrusion – are likely to be great when weighed against the disruption and publicity of formal actions including raids, arrests and prosecutions. In cross-border investigations, companies will need to devise due process safeguards to protect the rights of individuals and respect local law requirements. Ensuring local law specialists are instructed to work as part of a multidisciplinary team will be key.

Appendix 1

About the Authors

Hector Gonzalez
Dechert LLP

Hector Gonzalez advises corporations and executives on a wide range of matters, with a focus on complex commercial litigation, criminal and related civil and administrative matters, SEC and CFTC enforcement proceedings, and internal, grand jury and state attorneys general investigations. In addition, he regularly represents clients in all aspects of Foreign Corrupt Practices Act (FCPA) and Racketeer Influenced and Corrupt Organizations Act (RICO) matters.

Mr Gonzalez has been consistently recognised for his white-collar criminal defence practice and his securities and shareholder litigation practice by *The Legal 500 US*, which praises him as 'a great lawyer' in commercial litigation, having 'an extraordinary amount of expertise' in securities shareholder litigation, and being 'an excellent trial lawyer and strategic thinker who won't waste clients' time or money.' *Benchmark Litigation 2015* named Mr Gonzalez a Litigation Star for his white-collar defence practice and described him as 'one of the sharpest and most promising talents doing this work right now'.

Mr Gonzalez has significant trial experience, having tried more than 20 federal and state jury trials and argued more than 30 cases before federal and state appellate courts. Mr Gonzalez was previously an Assistant US Attorney in the US Attorney's Office for the Southern District of New York, where he served as Chief of the Narcotics Unit and was twice awarded the Department of Justice's Director's Award for Superior Performance.

Rebecca Kahan Waldman
Dechert LLP

Rebecca Kahan Waldman is a partner in the white-collar and securities litigation group. Ms Waldman focuses her practice on complex commercial and securities disputes with an emphasis on litigation involving the banking and financial services sectors, white-collar and

internal investigations, and e-discovery. She also has significant trial experience and has served as trial counsel in a number of federal, state and bankruptcy litigations.

Her significant representations include advising the former chief executive officer of registered futures commission merchant and broker dealer in civil litigations and congressional and regulatory inquiries arising out of bankruptcy of former employer; the former chief risk officer of Fannie Mae against securities fraud charges filed by the SEC in the Southern District of New York; individuals and companies in class action lawsuits alleging violations of federal securities laws; individuals and companies in investigations commenced by the SEC, CFTC, Department of Justice, state attorneys general and Congress; and The Bank of New York Mellon in all aspects of litigation and SEC and CFTC investigations relating to the bankruptcy of Sentinel Management Group.

Caroline Black
Dechert LLP

Caroline Black is a criminal defence and investigations lawyer focused on cross-border regulatory or internal investigations. She advises organisations, boards and audit committees on conducting investigations and interacting with relevant national authorities, including the Serious Fraud Office, HM Revenue and Customs and the police (and their overseas equivalents). Ms Black focuses her practice on the investigation and defence of business crimes, particularly matters involving corruption, money laundering, fraud and tax concerns. She has received awards for training and management and was also included in the 2015 edition of *Global Investigations Review*'s 'Women in Investigations' profile, which highlights 100 remarkable women from around the world for their accomplishments in this area of law.

William Fotherby
Dechert LLP

William Fotherby focuses his practice on white-collar and securities matters. He acts for companies and individuals faced with serious criminal charges, often brought by the prosecuting authorities of different jurisdictions simultaneously. Most often these charges involve bribery, corruption or securities fraud. He also provides advice to state governments about criminal prosecution strategy, asset recovery and mutual legal assistance.

Mr Fotherby has acted for foreign states and individuals in often high-profile extradition matters. He also has extensive knowledge of British Overseas Territories law.

Prior to joining the firm, Mr Fotherby worked as a barrister and solicitor at Meredith Connell, the Office of the Crown Solicitor for Auckland, New Zealand. In that role, he conducted numerous jury trials and other criminal hearings. He also represented the New Zealand government on immigration matters, parole and *habeas corpus* hearings, defamation suits and other regulatory matters. He has argued appeals in criminal and civil cases up to and including the New Zealand Supreme Court.

As part of Dechert's *pro bono* programme, he has helped a number of prisoners convicted of murder to challenge their convictions.

Dechert LLP
1095 Avenue of the Americas
New York, NY 10036-6797
United States
Tel: +1 212 698 3500
Fax: +1 212 698 3599
hector.gonzalez@dechert.com
rebecca.waldman@dechert.com

160 Queen Victoria Street
London
EC4V 4QQ
United Kingdom
Tel: +44 20 7184 7000
Fax: +44 20 7184 7001
caroline.black@dechert.com
william.fotherby@dechert.com

www.dechert.com

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISBN 978-1-912377-34-3