GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

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

SIXTH EDITION

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

2021

The Practitioner's Guide to Global Investigations

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

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

The Practitioner's Guide to Global Investigations

Sixth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Celeste Koeleveld

Acknowledgements

ABB Ltd

Addleshaw Goddard LLP

Anagnostopoulos

Association of Corporate Investigators

Baker McKenzie LLP

BCL Solicitors LLP

BDO USA, LLP

Blank Rome LLP

Booking.com

Brown Rudnick LLP

Cadwalader, Wickersham & Taft LLP

Claro y Cia

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Corker Binning

Cravath, Swaine & Moore LLP

Debevoise & Plimpton LLP

DLA Piper LLP

Fornari e Associati

Fountain Court Chambers

Fox Williams LLP

Freshfields Bruckhaus Deringer LLP

Gleiss Lutz

Goodwin

Herbert Smith Freehills

Homburger

Jenner & Block

Jones Day

Kingsley Napley LLP

Latham & Watkins

Linklaters LLP

McGuireWoods

Marval O'Farrell Mairal

Matheson

Mayer Brown

Meredith Connell

Mishcon de Reya LLP

Navacelle

Noerr

Nokia Corporation

Norton Rose Fulbright LLP

Outer Temple Chambers

Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pinsent Masons LLP

Rebaza, Alcázar & De Las Casas

Reed Smith LLP

Ropes & Gray LLP

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

Slaughter and May

Sullivan & Cromwell LLP

Trench Rossi Watanabe

Uría Menéndez Abogados, SLP

Walden Macht & Haran LLP

Willkie Farr & Gallagher LLP

Publisher's Note

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

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

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

The volumes

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

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

Online

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

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

Foreword

Mary Jo White

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

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

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

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

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

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

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

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

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

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

New York
November 2021
mjwhite@debevoise.com

Preface

The history of the global investigation

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

The Guide

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

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

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

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

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

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

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

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

Contents

11

Production of Information to the Authorities

Pamela Reddy, Kevin Harnisch, Katie Stephen, Andrew Reeves and Ilana Sinkin[1]

11.1 Introduction

The production of information to authorities is often rife with legal and practical issues that need to be tackled carefully but quickly. Taking control of the process and engaging with regulators early on can focus the information request and help to establish a positive and more productive relationship. In many cases, a regulator will welcome the assistance of the company and its advisers in scoping and prioritising the regulator's receipt of data (and this may result in significant cost savings for the company).

It is important to engage with the regulator as soon as possible and to establish its internal drivers and deadlines, as well as any immediate priorities within the data it has sought. Prioritising may provide more time to work on the broader production (while giving authorities what they need to progress their investigation and satisfy their stakeholders). Engaging with authorities early may also allow the company to find out more about the underlying investigation.

Approaching information requests methodically helps to ensure that all key issues are worked through. Immediate issues to consider include:

- whether the company is the subject of the investigation and any immediate consequences in terms of required notifications and internal communications;
- the powers under which the request is made (and whether what has been requested falls within those powers, including in terms of where it is located);

1 Pamela Reddy, Kevin Harnisch, Katie Stephen and Andrew Reeves are partners, and Ilana Sinkin is a senior associate, at Norton Rose Fulbright LLP.

- whether the information is required or merely requested (and whether the company wants to seek a compelled request to help deal with any potential issues arising from voluntary disclosure such as data privacy or confidentiality concerns);
- timing (focusing on what can be done within the requested time frame, however tight, tends to lead to a better outcome in terms of obtaining extensions);
- the precise scope of the request (and considering whether clarification or narrowing is required);
- what sources of data may need to be explored (including electronic devices in employees' possession) and the extent to which assistance from custodians may be required;
- the proposed approach to protecting privilege;
- any additional requirements triggered by the data request, such as in relation to data preservation or other reporting;
- to what extent the company plans to review all material before it is provided to the regulator or subsequently;
- where multiple regulators are involved, coordination and ensuring a consistent response and minimising duplication of effort; and
- the impact of local laws on the collection, review and production of data (including whether the process of responding will involve any issues arising from cross-border transmission of data).

Cost and proportionality are key issues in data productions. While most companies will want to be co-operative, it is also important that data is not needlessly collected, hosted, reviewed and produced. Data sources and volumes are ever increasing and seemingly small decisions (e.g., as to the number of custodians, date ranges or precise search terms) can have a significant impact on the overall cost of the production and ongoing hosting (as well as the usefulness of the data for the regulator). Where broad search terms are required or applied in the first instance, review of a sample of the results or a technology-assisted review might enable narrowing of the searches. Equally, the approach to privilege reviews can have a big impact on cost. In some circumstances, a non-exhaustive technology-driven process may be appropriate combined (in some jurisdictions) with putting in place a clawback agreement with the regulators.

The technical details are important when it comes to data collection. Time spent working through IT infrastructure, device history, the status of former employees' data, and so on, optimises collection and can help to reduce costs in the long term. It is also crucial that collection and production IT requirements are fully understood and that any uncertainties are flushed out to avoid document productions needing to be rerun later down the line.

Increasingly document and information requests cover not only documents and emails, but also other electronic records such as SMS, WhatsApp and similar messages and voice notes (which may be less easily searchable).

The move to increased remote working accelerated by the covid-19 pandemic has generated a greater volume and variety of potentially responsive electronic communications while also hindering the process of responding to information requests. Great care needs to be taken to ensure that all relevant data is preserved, including data and devices held off-site.

In this chapter we set out key considerations when responding to document requests from UK and US regulators and important issues to be considered when conducting reviews and making productions.

11.2 UK regulators

11.2.1 Powers of the Serious Fraud Office

The key power available to the Serious Fraud Office (SFO) is to require documents or information under a notice pursuant to section 2 of the Criminal Justice Act 1987 (CJA) (a section 2 notice).

The SFO can compel a person (individual or corporate) it has begun investigating[2] and any other person whom it believes may have information which is relevant to that investigation, to produce documents or information recorded in any form with respect to 'any matter relevant to the investigation'.[3] There is no 'right to silence' (although where an individual provides information during a compelled interview, that information cannot, except in very limited circumstances, later be used against that individual during a prosecution).

Failure to comply with a section 2 notice is a criminal offence that can result in imprisonment for a term of up to six months or a fine, or both.[4] The only defence is where there is a 'reasonable excuse' for the non-compliance but this is likely to be very narrowly construed. The key exception to the provision of documents is where documents are protected by legal professional privilege. The SFO has stated in its Corporate Co-operation Guidance[5] that it expects companies producing documents to obtain independent certification that withheld material is privileged, and it has indicated on various occasions that it views waiver of privilege as an indicator of co-operation (although it has stressed that it does not require waiver).

In February 2021, the UK Supreme Court ruled that section 2(3) of the CJA does not have extraterritorial effect.[6] This means that a section 2 notice cannot be used to compel a foreign company that does not carry on business in the United Kingdom to produce documents held outside the country. The SFO will have to obtain any such documents via mutual legal assistance (MLA).

---

2 The powers can also be used before the SFO has opened an investigation where it appears to the Director of the SFO that conduct that may constitute an offence under the UK Bribery Act 2010, ss.1, 2 or 6 may have taken place (CJA, s.2A).

3 CJA, s.2(2).

4 ibid., s.2(13).

5 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/corporate-co-operation-guidance/.

6 *R (KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2.

Although the section 2 powers are broad, the scope and timing of the response to section 2 notices is nearly always a matter of negotiation.

Powers of other authorities 11.2.2

Various other authorities may require documents to be produced. The powers of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) are dealt with in more detail below. The National Crime Agency (NCA) and Her Majesty's Revenue and Customs (HMRC) can require an individual to provide information, documents or communications in their possession pursuant to a disclosure notice issued under section 62 of the Serious Organised Crime and Police Act 2005 (SOCPA). A disclosure notice can be issued if it appears that there are reasonable grounds for suspecting that a relevant offence (such as failure to prevent facilitation of tax evasion or money laundering) has been committed and that any person has information relating to a matter relevant to the investigation of that offence that is likely to be of substantial value to that investigation. A person who fails to comply commits an offence under section 67(1) SOCPA and a conviction can result in fines or imprisonment of up to two years.

There are exceptions to the provision of documents for legally privileged documents and confidential banking information. Certain categories of material that a person cannot be required to provide are set out in the Police and Criminal Evidence Act 1984 (PACE).[7] There is also no right to silence in an interview compelled under section 62 SOCPA.

Where there has been failure to comply with a request under section 62 SOCPA, or where giving a notice under section 62 may be prejudicial to the investigation, under section 66 SOCPA, both HMRC and the NCA can apply before a magistrate for a search warrant.

The Proceeds of Crime Act 2002 also provides mechanisms, such as production orders, for obtaining documents.[8] In addition, there are various powers within PACE that allow authorities to search the premises for documents.

FCA and PRA 11.2.3

Compulsory requests 11.2.3.1

In its Enforcement Guide, the FCA states that its standard practice is to use statutory powers to require the production of information or documents.[9] The FCA and PRA both have a general power in support of their supervisory and enforcement functions[10] to compel the production of information and documents.[11] This allows the regulators to request in writing that 'author-

7 Police and Criminal Evidence Act 1984, s.11.

8 Proceeds of Crime Act 2002, s.345.

9 FCA Enforcement Guide [EG], EG 4.7.1.

10 EG 3.2.1.

11 Financial Services and Markets Act 2000 (FSMA), s.165.

ised persons'[12] or persons connected with authorised persons provide specified information or documents that are 'reasonably required' in connection with the regulator's statutory powers.[13] The definition of 'connected with' is broad and includes group members, parent undertakings and employees of authorised persons. The FCA and PRA can stipulate (1) the form in which the information is provided[14] and (2) that the information or document is verified or produced to be authenticated.[15]

The regulators also have separate powers for the production of information and documents in connection with investigations.[16] Depending on the matters being investigated, in addition to being able to require the production of relevant information and documents by the person under investigation or any connected person, the FCA and PRA may require another person to produce information or documents in specified circumstances. The FCA or PRA can also use its powers to assist an overseas regulator.[17]

A company may resist disclosure requested by the FCA or PRA using its compulsory powers, where (1) the relevant material is a 'protected item' (under the statutory definition within the Financial Services and Markets Act 2000 (FSMA))[18] or (2) the information or document is not within the scope of the request.

Failure to comply with the request may be treated as a 'serious form of non-cooperation' and as contempt of court and may give rise to a Principle or Conduct Rule breach.[19]

11.2.3.2 Voluntary production

The FCA Enforcement Guide explains that it will sometimes be appropriate to depart from the FCA's standard practice of using its statutory powers to obtain information and documents such as for suspects in criminal or market

12 Firms authorised by the FCA to provide regulated financial services as defined in FSMA, s.31.

13 See also FSMA, s.175.

14 ibid., s.165(5).

15 ibid., s.165(6).

16 ibid., s.167 (general investigations), s.168 (specific investigations), ss.171 to 173.

17 ibid., s.169; EG 3.7.

18 s.413 – '(2) "Protected items" means – (a) communications between a professional legal adviser and his client or any person representing his client which fall within subsection (3); (b) communications between a professional legal adviser, his client or any person representing his client and any other person which fall within subsection (3) (as a result of paragraph (b) of that subsection); (c) items which – (i) are enclosed with, or referred to in, such communications; (ii) fall within subsection (3); and (iii) are in the possession of a person entitled to possession of them. (3) A communication or item falls within this subsection if it is made – (a) in connection with the giving of legal advice to the client; or (b) in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings.'

19 EG 4.7.4 – the FCA may bring proceedings for breach of Principle 11, Statement of Principle 4 or FCA Code of Conduct Handbook (COCON) 2.1.3R.

abuse investigations.[20] In connection with the use of statutory powers to require the production of documents, the provision of information and the answering of questions regulated firms and certain individuals must be open and co-operative with the FCA and PRA when responding.[21] Regulated firms and approved persons such as senior managers are also expected to proactively disclose to the FCA or PRA anything of which the regulator would reasonably expect notice.[22] The FCA also encourages voluntary production of information such as reports from internal investigations.[23]

The level of co-operation is taken into account by the FCA and PRA when deciding whether to bring enforcement action and when determining any penalty. However, prior to making voluntary disclosure, firms should consider any other relevant obligations such as duties of confidentiality and data protection requirements.

FCA and PRA obligations 11.2.3.3

FSMA restricts the disclosure by the FCA or PRA of information relating to a firm's business where such information is confidential and has been received for the purposes of the authority's functions.[24] It is a criminal offence to make an unauthorised disclosure, but there are a number of exceptions, including where prescribed 'gateways' apply such as disclosure to overseas regulators.

Information Commissioner's Office 11.2.4

As data breaches become more prevalent and companies recognise the extent of potential liability following high-profile cases in 2020 involving British Airways and Marriott, considerations regarding the provision of information to regulators, enforcement agencies and other third parties are becoming increasingly important.

Following the submission of a personal data breach form, there are typically numerous rounds of questions from the Information Commissioner's Office (ICO) should it decide to investigate. The purpose of these questions

20 EG 4.7.1: 'In such a case, the interviewee does not have to answer but if they do, those answers may be used against them in subsequent proceedings, including criminal or market abuse proceedings.'

21 See the FCA's reminder in its Enforcement Guide at EG 4.7.2.

22 Principle 11 of the FCA's Principles for Businesses, Fundamental Rule 7 of the Prudential Regulation Authority's Fundamental Rules. There are a number of enforcement outcomes relating to breaches of these provisions; e.g., *The Bank of Tokyo Mitsubishi UFJ Limited and MUFG Securities EMEA plc*, February 2017, available at https://www.bankofengland.co.uk/news/2017/february/pra-imposes-fine-on-the-bank-of-tokyo-mitsubishi-ufj-limited-and-fine-on-mufg-securities-emea-plc, and Bank of Scotland plc, June 2019, available at https://www.fca.org.uk/publication/final-notices/bank-of-scotland-2019.pdf. In relation to senior managers see Senior Manager Conduct Rule SC4 in COCON 2.2.4R.

23 EG 3.1.2, EG 3.11.

24 FSMA, s.348.

is not only to understand more about the breach and establish whether the rights of data subjects have been adequately protected, but also to understand more about the company's technical and organisational measures at the time of the breach to assess whether the EU General Data Protection Regulation has been infringed. These requests for information are typically made on an informal basis. However, the ICO may compel the production of information via an information notice under section 142(1) of the Data Protection Act 2018 (DPA). Failure to comply can result in the issuance of a penalty notice under section 155(1)(b) DPA.

Companies should, however, be alive to the potential ramifications of disclosing certain information should subsequent litigation commence, for example in the form of third-party security provider disputes or class actions brought on behalf of data subjects. Companies at the outset of a data breach investigation should consider whether any documents produced could be protected by legal professional privilege (under section 143(4) DPA or common law) and to what extent companies can and should exercise that right. Carefully considering the privilege position is even more important in light of recent draft statutory guidance published by the ICO on 1 October 2020, which provides that the ICO may obtain privileged communications unrelated to data protection legislation in certain circumstances. Until this guidance has been approved by Parliament and put in practice, it remains to be seen whether there will be a significant departure from the ICO's current approach to privileged communications as set out in its Regulatory Action Policy.

Production of documents to other authorities, for example the NCA and FCA, also needs to be considered when investigating and managing large data breaches. The NCA's approach to companies that have suffered a cyberattack differs to its approach when investigating a company of wrongdoing where it seeks to bring a prosecution against the perpetrator. The NCA does not typically have the power to compel a company to co-operate with its investigation by producing documents or answering questions in this context, so it is the company's decision whether to engage with the NCA. In general, the NCA does not voluntarily provide information on a data-breach investigation to the ICO, and it is not a public authority for the purposes of the Freedom of Information Act 2000. However, companies should bear in mind that the ICO does have powers under Part 6 of the DPA to oblige third parties to respond, and material provided to the NCA could be made public in the event of a prosecution.

See Chapters 40 on data protection and 41 on cybersecurity

11.2.5 The Pensions Regulator

The Pension Schemes Act 2021 has introduced new information-gathering powers. It enables the Pensions Regulator to require by notice in writing a person likely to hold information relevant to the exercise of the regulator's

powers to attend an interview before the regulator.[25] Failure to attend the interview or to answer questions, without a reasonable excuse, is a criminal offence.[26] This new power is enforceable by a series of escalating fines of up to £10,000 a day.[27]

US regulators 11.3

In the United States, most federal agencies have statutory authorisation to issue administrative subpoenas to compel individuals and entities to produce documents and testimony without prior approval from a court or grand jury.[28]

The US Supreme Court has broadly upheld the use of administrative subpoenas (subpoenas issued by a federal agency without judicial oversight), holding that the government need only show that the administrative subpoena was issued in good faith.[29] In *United States v. Powell*, the Supreme Court articulated a four-factor test to evaluate whether a subpoena was issued in good faith: (1) the investigation is conducted pursuant to a legitimate purpose; (2) the information requested under the subpoena is relevant to that purpose; (3) the agency does not already have the information that it is seeking with the subpoena; and (4) the agency has followed the necessary administrative steps in issuing the subpoena.[30]

In general, federal courts may enforce administrative subpoenas, and refusal to obey a federal court order to comply with an administrative subpoena can result in a federal district court imposing contempt sanctions for non-compliance. In addition, some statutes authorise the court to assess civil penalties for non-compliance with a subpoena.[31]

While each federal agency has its own unique and statutory regulatory schemes for issuing administrative subpoenas, the US Department of Justice

25 Pensions Act 2004, s.72A(1) .

26 ibid., s.77(1A).

27 ibid., s.77A.

28 See, e.g., 15 U.S.C. § 78dd2(d)(2) (The US Department of Justice (DOJ) is granted statutory authority under the US Foreign Corrupt Practices Act 'to subpoena witnesses, take evidence and require the production of any books, papers, or other document'); 7 U.S.C. § 15 (The US Commodity Futures Trading Commission may 'subpoena witnesses, compel their attendance . . . and require the production of any books, papers, correspondence, memoranda, or other records that the Commission deems relevant or material to the inquiry'); Securities Act of 1933, Pub. L. No.73-22 (as amended), Sec. 19(b) (The US Securities and Exchange Commission may subpoena witnesses, take evidence and require the production of documentary evidence deemed relevant or material to an investigation under the Securities Act. The attendance of witnesses and production of documents may be required from anywhere in the United States or any territory at any designated place of hearing).

29 *United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 313 (1978).

30 379 U.S. 48 (1964).

31 See 42 U.S.C. § 9604(e) (authorising the court to assess civil penalties of up to US$25,000 for each day of continued non-compliance with subpoena issued under Comprehensive Environmental Response, Compensation, and Liability Act authority).

(DOJ) is the primary federal agency authorised to enforce federal law and defend the interests of the United States. The DOJ has oversight of several federal law enforcement agencies, including the Federal Bureau of Investigation, and is responsible for investigating instances of fraud and corruption. Section 248 of the Health Insurance Portability and Accountability Act 1996 for example, authorises the Attorney General – the chief lawyer of the US federal government and the leader of the DOJ– to issue subpoenas requesting 'production of certain documents and testimony in investigations related to 'any act or activity involving a federal health care offense'.[32]

In addition, the Inspector General Act 1978 created an Office of Inspector General (OIG) within several federal agencies. These OIGs also conduct investigations and may require, by subpoena, the production of documents and testimony to investigate potential fraud involving recipients of federal funding within their respective agencies. Inspectors General are intended to function independently of the agency head.

When producing documents or testimony to a federal agency the information must be accurate. In the United States, it is a criminal offence, punishable by imprisonment and a fine, to knowingly and wilfully make any materially false statement or document to a federal agency.[33] In addition, a person can be criminally prosecuted for perjury if he or she wilfully provides false testimony under oath to a US regulator.[34] Under the Fifth Amendment to the US Constitution, a natural person (not an entity) may refuse to provide information in response to a subpoena if that information may be self-incriminating.

The Freedom of Information Act (FOIA) generally requires government agencies to disclose information, including documents obtained from third parties, upon request. FOIA, however, contains a number of exceptions, allowing government entities to withhold information obtained in response to an administrative subpoena in certain circumstances. When providing information in response to government requests, the producing party should properly claim the appropriate exemptions from disclosure under FOIA.

11.3.1 Voluntary productions

Despite statutory authority to compel production, there are various reasons why federal agencies will seek voluntary productions from an individual or entity. For example, while the DOJ may issue a grand jury subpoena to 'a subject or a target of the investigation', DOJ attorneys are urged to secure information from

32 See 18 U.S.C.§3486(a)(1)(A)(i)(I).

33 18 U.S.C. § 1001 (Whoever knowingly and wilfully makes any materially false statement or writing or document in connection with any matter before the US government may be imprisoned and fined).

34 18 U.S.C. § 1621 (In certain cases, if any person wilfully provides information as true which he does not believe to be true is guilty of perjury).

a target of an investigation through voluntary means prior to obtaining a grand jury subpoena because a subpoena 'may carry the appearance of unfairness'.[35]

In addition, the DOJ has issued various policies providing incentives for companies and individuals to voluntarily disclose information. For example, the DOJ Criminal Division's Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy provides that the DOJ may decline to prosecute a company that (1) voluntarily self-discloses misconduct in an FCPA matter, (2) fully co-operates with the DOJ's investigation, and (3) remediates the misconduct in an appropriate and timely manner.[36] The DOJ's Criminal Division has expanded this policy beyond FCPA matters, including in cases involving healthcare and financial fraud.[37] Other agencies provide similar incentives for voluntary co-operation.

If a company is producing documents voluntarily, the company should pay considerable attention to potential disclosure of privileged information. Courts have held that the voluntary submission of privileged materials waives privilege in the United States, whereas a submission made under compulsion does not.[38] In assessing whether the disclosure of privileged documents to regulators was involuntary, courts consider a number of factors, including whether (1) the disclosure was made in response to a court order or subpoena or demand of a government authority, (2) the disclosing party would be subject to penalties if it failed to produce the documents, and (3) the disclosing party objected to the disclosure and asserted any available privilege protections over the documents.[39]

Privilege 11.4

Under English law, communications subject to legal professional privilege are protected. Subject to very narrow exceptions, third parties, including authorities, cannot compel disclosure of privileged information or documents. This common law protection is also broadly reflected in certain statutory provisions (such as section 413 FSMA), but these are not entirely consistent.

See Chapters 36 and 37 on privilege

35 US DOJ, Justice Manual § 9-11.150 (Justice Manual) ('before a known 'target' is subpoenaed to testify before the grand jury about his or her involvement in the crime under investigation, an effort should be made to secure the target's voluntary appearance').

36 Justice Manual § 9-47.120.

37 See, e.g., Deputy Assistant Att'y Gen. Matthew S Miner, U.S. Dep't of Justice Criminal Div., Remarks at the 5th Annual Global Investigations Review New York Live Event (27 September 2018), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division.

38 See *In re Vitamin Antitrust Litig.*, 2002 WL 35021999, at *28 (D.D.C. 23 January, 2002).

39 Id.

Under common law there are two types of legal professional privilege:

- Legal advice privilege protects confidential communications between a lawyer[40] and a client for the dominant purpose of giving or receiving legal advice. 'Client' is construed very narrowly: it includes only those individuals within the organisation who are authorised to give instructions and receive advice on the particular matter. The fact that an employee may be authorised to communicate with the lawyers does not make them the client for privilege purposes.
- Litigation privilege protects confidential communications between the client or lawyer (on the one hand) and third parties (on the other), or documents created by or on behalf of the client or lawyer, which come into existence once litigation is in contemplation or has commenced and which are for the dominant purpose of use in the litigation. Litigation can include other adversarial proceedings, but may not be triggered by a regulatory investigation.

Applying the relevant principles in practice and determining the scope of information that may be withheld from the authorities is often complex and contentious (for example in relation to emails with multiple addresses and regarding attachments). In addition, there are circumstances in which regulators may seek to challenge decisions on privilege or request disclosure of privileged material, such as where internal investigations have been conducted by corporates in relation to potential regulatory problems (to the extent privilege is claimed over documents created during the internal investigation or that set out its findings).

In some circumstances the company may wish to provide privileged material on the basis of a limited waiver (with the right to assert privilege against third parties such as civil litigants), but this must be done carefully and with the benefit of legal advice to avoid inadvertently losing privilege.

In the United States, the attorney–client privilege and work-product doctrine can act as powerful shields in protecting documents from disclosure to US regulators. Generally, the attorney–client privilege protects confidential communications between an individual and his or her attorney that are made for the purpose of obtaining or providing legal advice or assistance. The attorney work-product doctrine applies to documents and information that have been prepared in reasonable anticipation of future litigation, or potentially an enforcement action, as contrasted with documents that are prepared for ordinary business purposes.

After receiving a document request from a regulator, careful consideration should be given to potential privilege issues. Particular care needs to be taken with respect to privilege issues when an internal investigation is concurrent with

40 'Lawyer' includes English solicitors, barristers and foreign lawyers qualified to practise in their own jurisdictions (and their staff acting under their direction). It does not include non-legal professionals giving legal advice but does include in-house lawyers.

the document production. This is because during an investigation, documents will usually be created pertaining to all aspects of the investigation, including reports on strategy, notes from employee interviews, forensic accounting reports of the company's books and records, and reports on the ultimate investigation findings. The recipient of the document request and the lawyers involved should act with the utmost caution to best maintain privilege over the investigation documents, but they should also ensure that all non-privileged investigation documents responsive to the document request are provided.

Cross-border investigations and considerations 11.5

Introduction 11.5.1

The United Kingdom and the United States both have comprehensive systems concerning the production of documents through the use of mutual legal assistance treaties (MLATs) and other international agreements, such as extradition agreements. MLATs enable a prosecutor in one country to request a prosecutor from another to gather and provide information; this assistance can include testimony, transferring persons in custody, assisting in proceedings related to asset forfeiture, and any other form of assistance permitted under the laws of the two countries.

In the United Kingdom, co-operation with foreign regulators may (and often does) occur at the prosecutorial level, and the SFO in particular has well-established relationships with the DOJ, the Australian Federal Police, and its European counterparts. All MLAT requests for legal assistance from the United States are sent to a specialist office within the central authority.

The FCA and PRA also have memoranda of understanding (MOUs) with other national and international authorities. In addition, certain US federal agencies have MOUs or exchange letters with their foreign counterparts. For example, the US Treasury's Financial Crimes Enforcement Network has MOUs with financial intelligence agencies in many countries, including the United Kingdom. The US Securities and Exchange Commission (SEC) also has co-operative arrangements with non-US regulators to facilitate co-operation with its counterparts in other countries.[41]

Recent years have witnessed a number of large cross-border investigations; for example, the recent cross-border joint investigation into Airbus resulted in co-ordinated settlements with UK, US and French authorities. A US federal appellate court held in *United States v. Allen*, that evidence derived from compelled testimony in the United Kingdom could not be used in a criminal case in the United States, even if that testimony was lawfully obtained in the United Kingdom.[42] In that decision, the FCA and the DOJ were jointly investigating alleged manipulation of the LIBOR inter-bank lending rate by two former traders. The FCA interviewed two traders and provided their testimony

41 https://www.sec.gov/about/offices/oia/oia_coopfactsheet.htm.

42 *United States v. Allen et al.*, No. 16-898 (2nd Cir. 19 July 2017).

to a former banker who co-operated in the DOJ's case against the two traders in the United States. The Second Circuit held that the DOJ had failed to demonstrate that the compelled testimony from the two traders did not taint the banker's testimony against the traders in the grand jury proceeding and the trial, and overturned the convictions. The Second Circuit held that incriminating statements to non-US officials may only be used as evidence in criminal cases in the United States if made voluntarily and the use of the compelled testimony to the FCA as evidence in a US criminal trial would violate the defendants' Fifth Amendment right against self-incrimination.

Notwithstanding that the *Allen* case could raise an impediment to collaboration between US and UK authorities, one can expect co-operation and co-ordination to increase: regulators are increasingly working together to investigate and resolve issues; the ambit of extraterritorial jurisdiction is being continually expanded; and common global standards for effective compliance programmes (whose existence may be a legal or *de facto* defence)[43] are emerging. Practical points for a client facing a multi-jurisdictional or multi-regulator investigation include the need for:

- early consideration of which jurisdictions or authorities may be engaged (various factors such as money laundering legislation and international funds flow may make this number greater than it first appears);
- early and co-ordinated engagement with each authority;
- maintaining clear and comprehensive records relating to production; and
- getting legal advice in each jurisdiction, for example in relation to privilege and data protection.

11.5.2 Information outside the United Kingdom

The UK authorities (including the SFO and FCA or PRA) may seek international assistance from overseas authorities in connection with the exercise of a wide number of investigatory powers, including the production of data from sources and persons outside the United Kingdom. Their powers are contained in the Crime (International Co-operation) Act 2003 (CICA).

Under CICA, an MLA request can only be made if it appears to the investigating authority that there are reasonable grounds for suspecting that an offence has been committed. The request must relate to the obtaining of evidence 'for use in the proceedings or investigation'.[44]

Moreover, the SFO and FCA or PRA can make direct approaches to the relevant authorities in other jurisdictions to obtain evidence directly.

Following a recent UK Supreme Court decision, it is now established that, in addition to MLA, the SFO may also use its coercive powers[45] to compel a UK company to produce documents held outside the jurisdiction and also

43 For example, UK Bribery Act, s.7 provides for the defence of 'adequate procedures'.

44 Crime (International Co-operation) Act 2003, s.7(2).

45 Under CJA 1987, s.2.

compel a foreign company that carries on a business in the United Kingdom to produce documents held outside the jurisdiction.[46]

Under the Crime (Overseas Production Orders) Act 2019 certain UK authorities (including the SFO and FCA or PRA) are able to seek a court order (an overseas production order) to compel a person outside the United Kingdom to provide electronic data stored abroad where a designated international co-operation arrangement between the United Kingdom and a foreign state exists. The only such agreement currently in existence is between the United Kingdom and the United States.[47]

Brexit 11.5.3

Following the end of the transition period on 31 December 2020, the United Kingdom is no longer party to the reciprocal and mutual legal assistance provisions contained in EU law.

Requests for MLA between the Member States of the European Union and the United Kingdom are now based on cooperation through the Council of Europe 1959 Convention on Mutual Assistance in Criminal Matters and its two additional protocols, as supplemented by provisions agreed in Title VIII of the EU–UK Trade and Cooperation Agreement.

It seems likely that co-operation between the United Kingdom and the European Union will continue even though the transition period has now ended; although in the absence of new legal provisions, there may well be increased delays in effecting co-operation.

Requests into the United Kingdom 11.5.4

Under CICA, UK authorities may assist overseas authorities via formal MLA requests (including European investigation orders (EIOs)) or through direct information sharing. The UK Central Authority, which forms part of the

46 *R (on the application of KBR, Inc.) v The Director of the Serious Fraud Office* [2021] UKSC 2. At first instance the Administrative Court had held that any foreign company (whether or not it carried on business in the United Kingdom) could be compelled to produce documents where there was a 'sufficient connection between the company and the jurisdiction'. This was overturned by the UK Supreme Court. *In R (on the application of Tony Michael Jimenez) v. (1) First Tier Tax Tribunal and (2) Her Majesty's Commissioners for Revenue and Customs* [2019] Civ 51, the Court of Appeal applied the 'sufficient connection' test set out in the first instance decision in *KBR* in ruling that HMRC was authorised to serve a 'taxpayer notice' on a UK taxpayer resident overseas to obtain information about that individual's tax position. The Supreme Court in *KBR* distinguished *Jimenez* as being decided on factors not present in *KBR*.

47 'Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime' (3 October 2019), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

Home Office, is responsible for incoming MLA requests. Where an incoming request relates to serious or complex fraud, it will be sent directly to the SFO, which is able to use its section 2 powers to assist in obtaining material on behalf of a foreign authority.[48] UK authorities treat incoming MLA requests confidentially. Their practice is to neither confirm nor deny the existence of an MLA request to any third-party enquiry.

Any EIOs received by the United Kingdom after the end of the transition period are now processed as an MLA request.

The FCA and PRA also have the power under section 169 FSMA to assist foreign regulators when requested, including using their coercive powers of investigation.[49] The FCA's guidance confirms that, when deciding whether to use its investigative powers in this way, the FCA will initially consider whether it is able to assist without exercising its formal powers (by getting information voluntarily).[50] However, where this is not possible, in making a decision regarding the exercise of its powers, the FCA may give 'particular weight' to (1) the seriousness of the case, (2) the importance of the case to UK persons, and (3) the public interest. The regulator is not required to investigate the 'genuineness or validity' of a request or to 'second guess a regulator as to its own law and procedures'.[51] In its enforcement policy, the PRA states that it sees providing assistance to overseas authorities as an 'essential part' of the discharge of its functions.[52] Similarly, the FCA Enforcement Guide states that 'the FCA views co-operation with overseas counterparts as an essential part of its regulatory functions'.[53]

11.5.5 US cross-border investigations

US federal and state government agencies commonly share information obtained in an investigation with one another. For example, the DOJ and the SEC are authorised to enforce the FCPA, and they often work together in a coordinated investigation and to bring parallel proceedings.[54] Entities or individuals co-operating with both the DOJ and the SEC in an FCPA matter may be producing information to each agency simultaneously. Further, on

48 To safeguard the privilege against self-incrimination, the SFO requires an undertaking from the requesting authority that any evidence obtained from a person under the SFO's coercive powers will be used against that person in a prosecution.

49 FSMA, s.169(4) sets out the factors the FCA may take into account in deciding whether to exercise its investigative powers.

50 EG 3.7.4.

51 *Financial Services Authority v. Amro* [2010] EWCA Civ 123, a case concerning the FCA's predecessor.

52 Prudential Regulation Authority (PRA), Statement of Policy, 'The PRA's approach to enforcement: statutory statements of policy and procedure' (October 2019), s.6(3).

53 EG 2.6.1.

54 See, e.g., SEC Order, *In the Matter of Walmart Inc.*, File No. 3-19207 (20 June 2019); DOJ Non-Prosecution Agreement, *U.S. v. Walmart* (20 June 2019).

22 June 2020, the SEC and the DOJ Antitrust Division signed an MOU to foster co-operation in antitrust matters.[55]

There has been increased coordination among US regulators and non-US regulators. A number of countries, including the United Kingdom, Argentina, Brazil, France, Mexico, South Korea and Vietnam, have enhanced their anti-corruption enforcement laws and are working alongside the United States to investigate and prosecute bribery and corruption.

Therefore, it is important for entities or individuals facing liability in multiple jurisdictions to try to harmonise the substance of data requests where possible. The increasing cross-border nature of investigations underscores the need to consider the impact of privacy laws on data collection, review and productions in each jurisdiction. In addition, the increased sharing of information between regulators can impact decisions as to whether to self-disclose to certain regulators (and the order in which self-disclosures should be made).

Conclusion 11.5.6

Responding to information requests has become increasingly complex as the variety and volume of data has increased, data privacy laws have tightened and regulators are increasingly working together internationally. Dealing with information requests successfully requires adept management of the legal risks in all relevant jurisdictions and careful consideration of how best to advance the position of the company while balancing the cost and business impact of the production.

55 Memorandum of Understanding Between the Antitrust Division, Dep't of Justice and the Sec. and Exch. Comm'n Relative to Cooperation with Respect to Promoting Competitive Conditions in the Securities Industry (22 June 2020), available at https://www.sec.gov/files/ATR-SEC%20MOU-06-22-2020.pdf.

Appendix 1

About the Authors of Volume I

Pamela Reddy
Norton Rose Fulbright LLP

Pamela Reddy is a white-collar crime and investigations lawyer based in London. Pamela is widely recognised as one of the United Kingdom's most distinguished white-collar crime lawyers.

With more than 20 years' experience, Pamela is able to advise on the full spectrum of criminal and regulatory law and covers all stages of investigations, from the initial internal investigation and potential self-reporting, through to interviews under caution, all the way to defending clients in jury trials. She has also worked on several high-profile public inquiries and advised individuals facing sexual misconduct allegations, which surfaced amid the #MeToo movement.

Pamela is now a first-choice counsel to global companies and senior executives on domestic and cross-border fraud, bribery and corruption, market abuse and money laundering investigations. She frequently acts on some of the most serious, complex and high-profile cases involving UK and foreign regulators, including the SFO, NCA, CPS, FCA and DOJ.

Prior to joining the firm, she led a team at a boutique criminal law firm, advising on high-profile and media-sensitive general criminal matters and white-collar crime.

Pamela is recognised in *Financier Worldwide*'s 'Power Players in Investigations & White Collar Crime 2021', *Who's Who Legal*'s Global Leaders in Investigations 2020 and *Global Investigations Review* 'Top 100 Women in Investigations 2018'. Pamela features in the top tiers of a range of criminal law categories by the leading legal directories, in which she has been described as 'brilliant – she is extremely knowledgeable, has good technical skills and works tirelessly'.

Kevin Harnisch

Norton Rose Fulbright LLP

Kevin Harnisch is the US head of regulation, investigations, securities and compliance at the firm. He is a litigator who defends clients before the United States Securities and Exchange Commission (SEC), FINRA and other self-regulatory organisations, the Department of Justice, the US Commodity Futures Trading Commission, US Attorneys' offices and federal courts. He handles matters relating to securities enforcement defence, internal investigations and anti-corruption issues, and represents corporations (and their directors and officers), broker-dealers, hedge funds, private equity funds and investment banks.

Kevin served as a branch chief in the Division of Enforcement of the SEC, where he led cases regarding financial fraud, market manipulation, insider trading, the Foreign Corrupt Practices Act and municipal bond offerings.

Kevin has significant experience defending public companies in a wide array of government agency investigations. Those investigations often pertain to such issues as the accuracy of financial statements, undisclosed related-party transactions, the adequacy of internal controls, the FCPA and other anti-corruption laws, responses to whistleblowers, and potential insider trading.

He is also active in representing broker-dealers in various matters, including in anti-money laundering and suspicious activity reporting issues, market manipulation, order handling and best execution, managing conflicts of interest, the reasonableness of supervision, and the effectiveness of internal controls.

Katie Stephen

Norton Rose Fulbright LLP

Katie Stephen is a financial services and investigations partner based in London. She specialises in advising clients on contentious regulatory matters, including internal and external investigations and enforcement proceedings involving a variety of regulators including the FCA, PRA, SFO, HMRC and Ofgem, as well as those in other jurisdictions.

She has twice been seconded to the FCA as a legal adviser to its Regulatory Decisions Committee and she has acted on a number of high-profile cases, including market abuse proceedings against firms and individuals. Katie has also conducted a wide range of internal investigations for financial institutions and corporates, including advising on the regulatory implications and cross-border issues arising from these, and she is praised by clients for her 'investigatory talents' (*The Legal 500*).

Ilana Sinkin

Norton Rose Fulbright LLP

Ilana Sinkin is a senior associate in Norton Rose Fulbright's Washington, DC, office, where she focuses her practice on regulatory and government investigations, white-collar criminal defence, compliance and internal investigations for both corporations and individuals. Ilana has experience in a broad range of government and internal investigations, including investigations related to anti-corruption laws such as the US Foreign Corrupt

Practices Act and the UK Bribery Act, sanctions and export control, securities enforcement, insider trading, financial fraud, the False Claims Act and market manipulation.

Ilana also has experience designing anti-corruption compliance policies and procedures, designing investigative plans, preparing witnesses for interviews, assisting in document collections and productions, managing document reviews, preparing investigative reports, responding to subpoenas and participating in presentations to enforcement authorities, including the Department of Justice, the Office of Foreign Assets Control, the Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Department of Commerce, Bureau of Industry and Security.

Ilana is admitted to practise law in Virginia and the District of Columbia. She is also admitted to practise in the United States District Court in the Eastern District of Virginia.

Norton Rose Fulbright

Norton Rose Fulbright LLP
3 More London Riverside
London, SE1 2AQ
United Kingdom
Tel: +44 20 7283 6000
pamela.reddy@nortonrosefulbright.com
katie.stephen@nortonrosefulbright.com
andrew.reeves@nortonrosefulbright.com

Norton Rose Fulbright US LLP
799 9th Street NW, Suite 1000
Washington, DC 20001
United States
Tel: +1 202 662 0200
kevin.harnisch@nortonrosefulbright.com
ilana.sinkin@nortonrosefulbright.com

www.nortonrosefulbright.com

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-272-5