

Global Investigations Review

The Practitioner's Guide to Global Investigations

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

Fifth 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

Fifth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Tara McGrath

GIR
Global Investigations Review

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

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:

natalie.hacker@lbresearch.com

Enquiries concerning editorial content should be directed to the Publisher:

david.samuels@lbresearch.com

ISBN 978-1-83862-272-5

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

Acknowledgements

ADDLESHAW GODDARD LLP
ANAGNOSTOPOULOS
ASSOCIATION OF CORPORATE INVESTIGATORS
BAKER MCKENZIE LLP
BCL SOLICITORS LLP
BDO USA, LLP
BORDEN LADNER GERVAIS LLP
BROWN RUDNICK LLP
CADWALADER, WICKERSHAM & TAFT LLP
CLARO Y CIA
CLIFFORD CHANCE
CLOTH FAIR CHAMBERS
COOLEY LLP
CORKER BINNING
CRAVATH, SWAINE & MOORE LLP
DEBEVOISE & PLIMPTON LLP
DLA PIPER LLP
FORNARI E ASSOCIATI
FOUNTAIN COURT CHAMBERS
FOX WILLIAMS LLP
FRESHFIELDS BRUCKHAUS DERINGER
GLEISS LUTZ
GOODWIN
GÜN + PARTNERS

HERBERT SMITH FREEHILLS LLP
HOMBURGER
JAMES P LOONAM ESQ
JENNER & BLOCK
KINGSLEY NAPLEY LLP
LATHAM & WATKINS
LAW OFFICES OF PANAG AND BABU
LINKLATERS LLP
MARVAL O'FARRELL MAIRAL
MATHESON
MAYER BROWN
MCGUIREWOODS
MISHCON DE REYA LLP
NAVACELLE
NORTON ROSE FULBRIGHT LLP
OUTER TEMPLE CHAMBERS
PHILIPPI PRIETOCARRIZOSA FERRERO DU & URÍA – PPU
PINSENT MASONS LLP
RAJAH & TANN SINGAPORE LLP
REBAZA, ALCÁZAR & DE LAS CASAS
REED SMITH LLP
ROPES & GRAY LLP
SKADDEN, ARPS, SLATE, MEAGHER & FLOM (UK) LLP
SLAUGHTER AND MAY
SOFUNDE OSAKWE OGUNDIPE & BELGORE
SULLIVAN & CROMWELL LLP
TRENCH ROSSI WATANABE
URÍA MENÉNDEZ ABOGADOS, SLP
VON WOBESER Y SIERRA, SC
WALDEN MACHT & HARAN LLP
WILLKIE FARR & GALLAGHER LLP

11

Production of Information to the Authorities

**Pamela Reddy, Kevin Harnisch, Katie Stephen, Andrew Reeves
and Ilana Sinkin¹**

Introduction

11.1

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 investigators what they need to progress their investigation and satisfy their stakeholders). Engaging with investigators 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);
- 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 concerns);

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

- 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 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 of the material it is providing to the regulator;
- where multiple regulators are involved, co-ordination and ensuring a consistent response and minimising duplication of effort to the extent possible; 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 (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. It is also crucial that collection and production IT requirements are fully understood and that any uncertainties are flushed out to avoid further document productions later down the line.

Increasingly document and information requests cover not only documents and emails, but also other electronic records such as WhatsApp messages and voice notes (which may be less easily searchable). Recent increased remote working resulting from the covid-19 pandemic is likely to have generated a greater volume and variety of potentially responsive electronic communications while also hindering the process of responding to information requests.

In this chapter we set out key considerations regarding UK and US regulators relating to document requests and important issues to be considered when making productions.

UK regulators

11.2

Powers of the Serious Fraud Office

11.2.1

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 investigating² 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 As set out in the SFO's Corporate Co-operation Guidance, this may include interviews of individuals in relation to compliance programmes, including compliance officers. 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 '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 Guidance⁵ 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 September 2018, it was held that section 2(3) of the CJA has certain extra-territorial effect.⁶

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 because ultimately the SFO, like any investigating authority, is focused on obtaining the most relevant material.

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 which may constitute an offence under sections 1, 2 or 6 of the UK Bribery Act 2010 may have taken place (Section 2A CJA).

3 Section 2(2) CJA.

4 Section 2(13) CJA.

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

6 *R (on the application of KBR Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2012 (Admin).

11.2.2 Powers of other authorities

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 cheating the public revenue, 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.

As with powers under the CJA, there are exceptions to the provision of documents for documents protected by legal professional privilege and confidential banking information. Certain categories of material that a person cannot be required to provide are set out in 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.

11.2.3 FCA and PRA

11.2.3.1 Compulsory requests

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 functions¹⁰ to compel the production of information and documents.¹¹ This allows the regulators to request in writing that 'authorised persons'¹² or persons connected with authorised persons provide specified information or documents

7 s.11 Police and Criminal Evidence Act 1984.

8 s.345 Proceeds of Crime Act 2002.

9 EG 4.7.1.

10 EG 3.2.1.

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

12 Firms authorised by the FCA to provide regulated financial services as defined in s31 FSMA.

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; and (2) that the information or document is verified or produced to be authenticated.

The regulators also have separate powers for the production of information and documents in connection with investigations.¹⁴ 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.¹⁵

A company may resist disclosure requested by the FCA or PRA using its compulsory powers: (1) where the relevant material is a ‘protected item’ (under the statutory definition within the Financial Services and Markets Act 2000 (FSMA));¹⁶ or (2) where the information or document is not within the scope of the written request.

If a firm or individual does not comply with a request for information or documents made by the FCA using its statutory powers, this may be treated by the FCA as a ‘serious form of non-cooperation’ and as contempt of court and may give rise to a Principle or Conduct Rule breach.¹⁷

Voluntary production

11.2.3.2

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 abuse investigations.¹⁸ The Enforcement Guide reminds regulated firms and individuals that they must be open and co-operative with the FCA¹⁹ and firms and senior manag-

13 See also s.175 FSMA.

14 s.167 (general investigations), s.168 (specific investigations), s.171 to s.173 FSMA.

15 s.169 FSMA, EG 3.7.

16 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.’

17 EG 4.7.4 – the FCA may bring proceedings for breach of Principle 11, Statement of Principle 4 or COCON 2.1.3R.

18 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.’

19 EG 4.7.2.

ers are expected to disclose to the FCA or PRA appropriately anything of which that regulator would reasonably expect notice.²⁰ The FCA also encourages voluntary production of information such as reports from internal investigations.²¹

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

11.2.3.3 FCA and PRA obligations

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.²² 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 to assist them to carry out their functions.

11.2.4 Information Commissioner's Office

As data breaches become more prevalent and companies recognise the extent of potential liability following recent high-profile cases involving British Airways and Marriott,²³ considerations regarding the provision of information to regulators, enforcement agencies and other third parties are becoming increasingly important.

After a large data breach, investigations by the Information Commissioner's Office (ICO) can be lengthy, resource-consuming and invasive for a company. Following the submission of a personal data breach form, there are typically numerous rounds of questions from the ICO should it decide to investigate. The purpose of these questions is not only to understand more about the breach and establish whether the rights and freedoms of data subjects have been adequately considered and 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

20 Principle 11 of the FCA's Principles for Businesses, Fundamental Rule 7 of the PRA's Fundamental Rules – there are a number of enforcement outcomes relating to breaches of these provisions, for example *The Bank of Tokyo Mitsubishi UFJ Limited and MUFG Securities EMEA plc*, February 2017, available at <https://www.bankofengland.co.uk/news/2017/february/pr-imposes-fine-on-the-bank-of-tokyo-mitsubishi-ufj-limited-and-fine-on-mufg-securities-emea-plc>. See also Rule SC4 in COCON 2.2.4R.

21 EG 3.1.2, EG 3.11.

22 s.348 FSMA.

23 See ICO Penalty Notice to British Airways plc of 16 October 2020, available at <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> and ICO Penalty Notice to Marriott International Inc of 30 October 2020, available at <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf>.

compel the production of information via an information notice under section 142(1) of the Data Protection Act 2018 (DPA). Failure to comply with an information notice 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.

Production of documents to other enforcement agencies and 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 (FOIA) 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

The Pensions Regulator

11.2.5

The Pension Schemes Bill (HL 2019-21) seeks to create two new criminal offences in respect of the operation of pension schemes.²⁴ The Pensions Regulator will be given powers to require by written notice any person who holds or is likely to hold information relevant to the exercise of the Pensions Regulator's functions to answer questions and provide explanations in respect of any of the matters specified in the notice. It will become a criminal offence to neglect or refuse, without reasonable excuse, to attend before the Pensions Regulator as required in the notice or to neglect or refuse to answer a question or provide an explanation in respect of a matter specified in the notice when attending before the Pensions Regulator.²⁵

²⁴ The Pension Schemes Bill, clause 107: adding ss.58A and 58B to the Pensions Act 2004.

²⁵ Clause 110, adding s.72A to the Pensions Act 2004.

11.3 US regulators

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.²⁶ In addition, the Inspector General Act 1978 (IGA) created an Office of Inspector General (OIG) within several federal agencies. These OIGs also conduct investigations within their respective agencies and investigate potential fraud involving recipients of federal funding. Inspectors General are intended to function independently of the agency head.

While each federal agency has its own unique and statutory regulatory schemes for issuing subpoenas, the US Department of Justice (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. For example, Section 248 of the Health Insurance Portability and Accountability Act 1996 (HIPAA) authorises the Attorney General to issue subpoenas requesting 'production of certain documents and testimony in investigations related to 'any act or activity involving a federal health care offense.'²⁷

The US Supreme Court has broadly upheld the use of administrative subpoenas, holding that the government need only show that the administrative subpoena was issued for a lawfully authorised purpose and sought information relevant to the agency's inquiry.²⁸ For example, 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 it is seeking with the subpoena; and (4) the agency has followed the necessary administrative steps in issuing the subpoena.²⁹

In general, federal courts may enforce administrative subpoenas, and refusal to comply with an administrative subpoena can result in a federal district court

26 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 (FCPA) '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).

27 See 18 U.S.C. § 3486(a)(1)(A)(i)(I).

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

29 379 U.S. 48 (1964).

imposing contempt sanctions for non-compliance. In addition, some statutes authorise the court to assess civil penalties for non-compliance with a subpoena.³⁰

When producing documents or testimony to a federal agency the information should 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.³¹ In addition, a person can be criminally prosecuted for perjury if he or she wilfully provides false testimony under oath to a US regulator.³² 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. The 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 exemptions from disclosure under the FOIA.

Voluntary productions

11.3.1

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 a target of an investigation through voluntary means prior to obtaining a grand jury subpoena because a subpoena 'may carry the appearance of unfairness.'³³

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) timely and appropriately remediates the misconduct.³⁴ The DOJ's Criminal Division has expanded this policy beyond FCPA mat-

30 See 42 U.S.C. §9604(e) (authorising the court to assess civil penalties of up to \$25,000 for each day of continued non-compliance with subpoena issued under CERCLA authority).

31 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).

32 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).

33 U.S. Dep't of Justice, Justice Manual § 9-11.150 (J.M.) ('[B]efore 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').

34 J.M. § 9-47.120.

ters, including in cases involving healthcare and financial fraud.³⁵ Other agencies provide similar incentives for voluntary co-operation.

11.4 Privilege

See Chapters 36
and 37 on
privilege

Under English law, communications subject to legal professional privilege are protected. Subject to very narrow exceptions, third parties, including regulators and law enforcement agencies, 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.

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

- Legal advice privilege protects confidential communications between a lawyer³⁶ and a client for the dominant purpose of giving or receiving legal advice. ‘Client’ is construed very narrowly: only those individuals within the organisation 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 client or lawyer (on the one hand) and third parties (on the other), or other documents created by or on behalf of the client or his lawyer, which come into existence once litigation is in contemplation or has commenced and which is 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 the findings).

In some circumstances the company may wish to provide privileged material on the basis of a limited waiver (i.e., 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.

35 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-divisionhttps://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division>.

36 ‘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.

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 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 (including providing items in possession of government departments), and any other form of assistance permitted under the laws of the two countries. Assistance through MLATs is provided routinely.

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 EU and other 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 to exchange information. For example, the US Treasury’s Financial Crimes Enforcement Network (FinCEN) 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.³⁷

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.³⁸ 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.³⁹ 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 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)⁴⁰ are emerging. There have been reports, however, of disagreements between the US and UK authorities in relation to the *Unaoil* case.⁴¹

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 (including all prior steps in relation to data and the individuals involved) with an awareness of the additional time large cross-border investigations may take; and
- getting legal advice in each jurisdiction, for example in relation to privilege and data protection.

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

38 The combined penalties totalled \$3.9 billion, making it the largest anti-corruption settlement in history.

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

40 For example, s.7 UKBA provides for the defence of 'adequate procedures'.

41 *Serious Fraud Office v. Ake and Others* [2020] at Southwark Crown Court.

Information outside the United Kingdom

The UK authorities (including the SFO and FCA/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 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’.⁴²

Among most EU Member States European investigation orders (EIOs) now allow streamlined access to evidence and information in criminal investigations. In particular a requested authority has 30 days to accept a request and 90 days to comply.

Moreover, the SFO and FCA or PRA can make direct approaches to the relevant authorities in other jurisdictions to obtain evidence directly to get information from those regulators (i.e. under gateways) or to ask them to use their powers against third parties.

In addition to MLA, the SFO, as previously mentioned, may also use its coercive powers⁴³ to compel a UK company to produce documents held outside the jurisdiction and also compel a foreign company to produce documents held outside the jurisdiction where there is a ‘sufficient connection between the company and the jurisdiction’.⁴⁴

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 (OPO)) 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 agreement currently in existence is between the United Kingdom and the United States; therefore currently an OPO may only be granted in respect of electronic data stored in the United States.⁴⁵

42 s.7(2) CICA.

43 Under s.2 CJA 1987.

44 *R (on the application of KBR Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2012 (Admin). This decision is currently on appeal to the UK Supreme Court. Subsequently 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 *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.

45 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 of 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<https://assets>.

11.5.3 **Brexit**

When the transition period ends on 31 December 2020, if no further provisions are agreed the United Kingdom will cease to benefit from the reciprocal and mutual legal assistance provisions contained in EU law, including the EIO.

In its political declaration on 17 October 2019, the United Kingdom articulated its vision of a future partnership with the European Union, asserting that there would be ‘comprehensive, close, balanced and reciprocal law enforcement and judicial co-operation in criminal matters.’⁴⁶ However, unless specific provision is agreed after 31 December 2020 the United Kingdom will no longer be able to benefit from EIO co-operation.⁴⁷

It seems likely that in any event UK/EU co-operation will continue at a substantial and meaningful level beyond the end of the transition period, although in the absence of new legal provisions, there may well be increased delays in effecting co-operation.

11.5.4 **Requests into the United Kingdom**

Under CICA, UK authorities may assist overseas authorities via formal MLA requests (including EIOs) or through direct information sharing. The UK Central Authority, which forms part of the 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 documentation and data on behalf of a foreign authority.⁴⁸ UK authorities, including the SFO, treat incoming MLA requests confidentially. Their practice is to neither confirm nor deny the existence of an MLA request to any third-party enquiry.

The FCA and PRA also have the power under section 169 FSMA to assist foreign regulators when requested to so, including using its coercive powers of investigation.⁴⁹ The FCA’s guidance confirms that, when deciding whether to use its

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_Counteracting_Serious_Crime.pdf

46 Paras. 80 and 81 of the political declaration, available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840656/Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom.pdf Paragraphs 80 and 81 of the political declaration, available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840656/Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom.pdf

47 If no further provision is made, the United Kingdom can fall back on the European Convention on Mutual Legal Assistance in Criminal Matters 1959 regarding Mutual MLA with the European Union.

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

investigative powers in this way, the FCA will initially consider whether it is able to assist without exercising its formal powers (for example, 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 case’s importance 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

US cross-border investigations

11.5.5

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 it is not uncommon for the two agencies to work together in a coordinated investigation and to bring parallel proceedings.⁵³ 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 22 June 2020, the SEC and the DOJ Antitrust Division signed an MOU to foster co-operation in antitrust matters.⁵⁴

In addition to US regulators working together domestically, 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).

⁵⁰ EG 3.7.4.

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

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

⁵³ 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).

⁵⁴ 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>.

11.5.6 Conclusion

Responding to information requests has become increasingly complex as the variety and volume of data has increased, data privacy laws have tightened and regulators have increasingly worked 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.

Appendix 1

About the Authors of Volume I

Pamela Reddy

Norton Rose Fulbright LLP

Pamela Reddy is a white-collar crime and investigations partner based in London. She has over 20 years' experience as a criminal lawyer advising senior individuals and companies on all aspects of domestic and international investigations and the criminal process. Pamela regularly deals with a wide range of regulators, particularly the SFO, CPS and FCA in the United Kingdom, as well as overseas regulators.

Pamela was previously a partner at a criminal boutique firm and has diverse sector experience including managing multiple high-profile cases. For example, Pamela represented a senior executive of Rolls-Royce in the SFO investigation. She has worked with many of the global banks and senior executives on LIBOR and EURIBOR investigations. Pamela was engaged by a suspect in the phone hacking allegations at the Old Bailey and worked on cases involving allegations following the #MeToo campaign, as well as advising a number of high-profile individuals on allegations arising from the Jimmy Savile investigation.

Pamela is profiled in *Global Investigations Review's* 100 Women in Investigations 2018 and as Who's Who Legal Global Leader in Investigations 2020. *Chambers 2020* reported 'she is 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 attorney's 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*).

Andrew Reeves

Norton Rose Fulbright LLP

Andrew Reeves is a dispute resolution and investigations lawyer based in London.

Andrew represents corporates, financial institutions and senior executives in relation to a range of major regulatory and criminal investigations and proceedings including those brought by the UK SFO, NCA, FCA and PRA, as well as the US Department of Justice and the Securities and Exchange Commission, and various local regulators.

Andrew conducts internal investigations and due diligence for corporates and financial institutions, with a focus on bribery and corruption, fraud and money laundering. Andrew has worked on matters relating to Europe, Eurasia, Africa, India, China, South-East Asia, and South and Central America.

Andrew has experience of running complex money laundering investigations and a range of Proceeds of Crime Act work. Andrew also advises on major commercial litigation and disputes, usually multi-jurisdictional matters with elements of fraud.

In 2012 Andrew was seconded to a major global corporate, where he handled a range of litigation, investigations and regulatory matters.

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 anticorruption 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 anticorruption 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 LLP

3 More London Riverside

London, SE1 2AQ

United Kingdom

Tel: +44 20 7283 6000

pamela.reddy@nortonrosefulbright.com

kevin.harnisch@nortonrosefulbright.com

katie.stephen@nortonrosefulbright.com

andrew.reeves@nortonrosefulbright.com

ilana.sinkin@nortonrosefulbright.com

www.nortonrosefulbright.com/en-gb

an LBR business

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

ISBN 978-1-83862-272-5