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

5

Beginning an Internal Investigation: The UK Perspective

Jonathan Cotton, Holly Ware and Ella Williams[1]

5.1 Introduction

Company investigations arise from a diverse range of sources: from internal issues such as employee allegations, whistleblowing, supplier or customer complaints and audit findings, to external triggers such as reports in the press, on blogs and on social media, allegations in third-party litigation and approaches from regulators or other authorities, who may independently have uncovered an issue.

The focus of this chapter is on the factors relevant to a company's decision whether, when and how to launch an internal investigation, and to highlight key considerations in conducting the early stages of an internal investigation. These decisions are often made under significant time pressure, and with only limited information, but they can have serious repercussions.

5.2 Whether to notify any relevant authorities

See Chapter 3 on self-reporting

A key initial question when a potential issue comes to light is whether to notify any relevant authorities – which is likely, in turn, to impact several aspects of the internal investigation. Whether a notification is required or desirable will turn on the regulatory status of the company or the individuals uncovering the issue, the expectations of the relevant authorities and the issue itself.

Firms regulated by the Financial Conduct Authority (FCA) are under a duty to deal with their regulators openly and co-operatively and to disclose appropriately anything relating to them of which the FCA would reasonably

1 Jonathan Cotton and Holly Ware are partners and Ella Williams is senior counsel at Slaughter and May. The authors would like to thank Anna Lambourn, a professional support lawyer at the firm, for her assistance in preparing this chapter.

expect notice.[2] The FCA Handbook sets out a non-exhaustive list of situations where a firm is under an explicit duty to notify.[3] Although the timing of the notification will depend on the circumstances, the FCA expects a firm to discuss relevant matters with it 'at an early stage, before making any internal or external commitments', and in certain cases the notification obligation can be immediate.[4] Dual-regulated firms owe similar obligations to the Prudential Regulation Authority.[5]

Obligations to notify may also arise under anti-money laundering legislation. Persons working in the 'regulated sector' (a wider concept than just firms regulated by the FCA) must submit (subject to certain limited exceptions) a suspicious activity report (SAR) to the National Crime Agency in respect of information that comes to them in the course of their business if they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, or even just attempting the latter.[6] Even if a person does not work in the 'regulated sector', they may still need to make a SAR and an accompanying application for a 'defence against money laundering' to avoid the risk of committing a money laundering offence if they suspect that property they are dealing with is in some way criminal.[7]

Other notification requirements may arise under the rules of professional bodies[8] or under data privacy legislation.[9]

While there is no general legal obligation to report crime to the authorities, it may be in a company's interests to self-report suspicions of criminal conduct

2 Financial Conduct Authority (FCA) Handbook, PRIN 2.1.1R, Principle 11. Individuals subject to the FCA's individual conduct rules are also subject to equivalent obligations under FCA Handbook, Code of Conduct (COCON) 2.1.3 and COCON 2.2.4.

3 FCA Handbook, SUP 15.3.

4 ibid.

5 Prudential Regulation Authority (PRA) Rulebook, Notifications, Rule 2. (A dual-regulated firm is a firm that is a 'bank, a building society or a UK designated investment firm', FCA Handbook, SYSC 19 D.) The equivalent for PRA-authorised persons within the meaning of s.2B(5) Financial Services and Markets Act 2000 (FSMA) is Fundamental Rule 7 of the PRA Rulebook: A firm must deal with its regulators in an open and cooperative way and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice.

6 Proceeds of Crime Act 2002, ss.330 and 331 and Terrorism Act 2000, s.21A. 'Regulated sector' is defined in the Proceeds of Crime Act 2002, Schedule 9.

7 Proceeds of Crime Act 2002, ss.335 and 338.

8 For example, firms of solicitors have an obligation to report certain matters to the Solicitors Regulation Authority (SRA) (see, for example, Rule 3 (Cooperation and Accountability), Code of Conduct for Firms, SRA Standards and Regulations) and accountants regulated by the Institute of Chartered Accountants in England and Wales are subject to a reporting obligation under Disciplinary Bye-laws 9.1 and 9.2.

9 For example, there could be a requirement to notify the Information Commissioner's Office if a personal data breach may have occurred (see Regulation (EU) 2016/679 (General Data Protection Regulation), Article 33; Data Protection Act 2018, s.67).

to the Serious Fraud Office (SFO). The Deferred Prosecution Agreements Code of Practice (the DPA Code) states that it will be a public interest factor against prosecution if a company self-reports 'within a reasonable time of the offending coming to light';[10] a point that has been strongly endorsed by the courts in the DPA judgments handed down to date,[11] and which is reflected in the SFO's 'Corporate Co-operation Guidance' and the 'Deferred Prosecution Agreements' chapter in its Operational Handbook.[12] It has been acknowledged by the Director of the SFO that 'reasonable time' allows a company to conduct at least a preliminary investigation into a potential issue before self-reporting.[13]

See Chapters 3 on self-reporting to authorities and 23 on negotiating global settlements

Finally, certain companies will need to consider whether they are required (both at the outset of the investigation and on an ongoing basis) to make a disclosure to the market in relation to the potential issue that has come to light. If a market disclosure is required then it is easier to conclude that the company should also inform the relevant authorities.[14]

5.3 Whether and when to launch an internal investigation

Conducting an investigation is not without risk, and the risks should be considered carefully before an internal investigation starts. Once begun, an investigation can be difficult to stop or limit without damaging the company's credibility.

There can be a significant number of advantages to undertaking an internal investigation, including, principally, the ability to gain a better understanding of the facts to allow for more informed decision-making and the exploration

10 Deferred Prosecution Agreements Code of Practice, para. 2.8.2(i).

11 See, e.g., *Serious Fraud Office v. Standard Bank Plc (now known as ICBC Standard Bank Plc)* [2016] Lloyd's Rep FC 102, at para. 14; *Serious Fraud Office v. Tesco Stores Ltd* [2019] Lloyd's Rep FC 283, at paras. 66 and 117; *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at para. 47; *Serious Fraud Office v. Airline Services Limited* [2020] 10 WLUK 606, at para. 52; *Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep FC Plus 27, at para. 35.

12 Serious Fraud Office (SFO) Operational Handbook, Corporate Co-operation Guidance, August 2019, p. 1 (co-operation includes 'identifying suspected wrongdoing and criminal conduct . . . reporting this to the SFO within a reasonable time of the suspicions coming to light') and Deferred Prosecution Agreements, October 2020 ('[v]oluntary self-reporting suspected wrongdoing within a reasonable time of those suspicions coming to light is an important aspect of co-operation').

13 In a speech on 3 April 2019, Lisa Osofsky, Director SFO, said that companies 'have a duty to their shareholders to ensure allegations or suspicions are investigated, assessed and verified, so they understand what they may be reporting before they report it': available at https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/.

14 If applicable and the findings constitute inside information under the EU Market Abuse Regulation (transcribed into UK law via the European Union (Withdrawal) Act 2018 (as amended), as supplemented by The Market Abuse (Amendment) (EU Exit) Regulations 2019 (UK MAR)), the issuer would need to make such a disclosure. (UK MAR, Article 17(1): the issuer shall inform the public as soon as possible of inside information which directly concerns the issuer).

of possible defences, and to increase a company's ability to react effectively to any external investigations or adverse publicity. There can also be significant financial benefits if the results of the investigation allow the company to apply for leniency or immunity (principally available in the competition sphere) or to self-report and co-operate with an external investigation to gain a discount on a potential future financial penalty (or avoid prosecution altogether). Undertaking an internal investigation can also help to demonstrate that a company has adequate procedures and a corporate culture that takes compliance seriously, with wider benefits should the company's compliance framework later be evaluated. Linked to this, an internal investigation can also allow for proper remediation and the implementation of compliance enhancements that might help to avoid similar issues arising in future.

Sometimes, the factors in favour of conducting an internal investigation are acute. For example, where a company has to investigate to comply with its regulatory obligations (for instance the FCA Principles for Businesses)[15] or for directors to comply with their fiduciary and other statutory or common law duties.[16] A company may also have existing internal corporate governance codes or compliance policies that mandate an investigation. On the other hand, authorities have been known to request that companies do not conduct an internal investigation at all (for instance if it risks employees being 'tipped off' that they are under investigation, denying the authority the chance to monitor the relevant individuals covertly). Indeed, the FCA has stated that: 'Whether and how a firm investigates internally must now be looked at from the point of view of whether doing so will assist or inhibit the FCA's investigation.'[17]

There are, however, a number of potential downsides to conducting an internal investigation, which may in certain circumstances lead a company to decide not to investigate. These downsides include the potentially high costs and resource requirements of an investigation (including distraction from business as usual) and the reputational risk that might occur should the investigation become public. An investigation may, depending on its outcome, mean that companies have to notify stakeholders (such as insurers, auditors, lenders – particularly where the facts may constitute an event of default – and third-party customers), or make a disclosure to the market. There is also the risk that the internal investigation might result in the creation of non-privileged documents that could assist regulators, prosecutors or potential civil claimants (such as customers or shareholders), to the detriment of the company, and the risk that the investigation might uncover misconduct beyond the scope of the initial allegation.

15 FCA Handbook, PRIN 2.1.1R.

16 See, in particular, Companies Act 2006, ss.171 to 177.

17 Speech by Jamie Symington, then Director in Enforcement – Wholesale, Unauthorised Business and Intelligence, FCA (5 November 2015), available at https://www.fca.org.uk/news/speeches/internal-investigations-firms. See also FCA Handbook, Enforcement Guide (EG) 3.11.7.

When deciding whether and when to conduct an internal investigation, companies will also consider whether to instruct external legal counsel to advise on or conduct the investigation. In addition to providing investigations expertise and additional personnel, the engagement of external counsel can also bolster the independence of the investigation, which is important in a criminal or regulatory context, and provide an external viewpoint to balance the views of internal stakeholders. Engaging external counsel also increases the likelihood that privilege may apply to investigation documents.

5.4 Oversight and management of the investigation

One of the first issues to address at the outset of an internal investigation is to put in place an appropriate and robust governance structure, including who will have day-to-day management of the investigation and whom they will report to. The structure chosen will vary depending on the company and the issue.

Day-to-day management of the investigation is often given to the internal legal or compliance team, who will, therefore, likely be the 'client' for the purposes of instructing external legal counsel, with a consequent effect on the analysis of if and when legal advice and litigation privilege may arise. In any case, it will be important for potentially implicated individuals to be excluded from the investigation team, which should be kept under review in case additional individuals are implicated as a result of information that comes to light during the investigation. Where external advisers have been brought in to conduct an independent review, it may also be appropriate to limit the ability of the client to instruct or influence the review beyond clearly defined parameters, to preserve this independence. Further, if the issue under investigation arose as a result of whistleblowing, it will be important to bear in mind the rights of the whistleblower when designing the governance structure, particularly if the whistleblower has requested anonymity.

See Chapter 36 on privilege

See Chapter 19 on whistleblowing

The question of whom the investigation team will report to will often be determined by a company's existing corporate governance structure and framework of delegated authorities, and it is common for the investigation team to report to the board as a whole or the audit committee. However, in certain cases the company may choose to constitute a specific review body, such as a special subcommittee of the board or a panel of senior employees and external advisers. In such cases, the terms of reference of this body will need to be clearly defined, including what matters are to be referred to it, what powers it holds and how it is to interact with existing governance bodies in the company.

Where, as is common, the issue involves subsidiaries (some of which may not be wholly owned), it may be necessary to consider and reflect corporate separateness in the governance structure, such as reporting to the boards of those subsidiaries.

Whatever governance structures are established, it will be important to keep them under review and be able to amend them if new issues arise.

Scoping the investigation 5.5

A well-defined scope, reflected in written terms of reference and an investigation plan, helps to ensure that the objectives of the investigation are clear and to avoid a wide-ranging, unfocused investigation, with consequent wastage of time, resources and cost. Clearly recording the scope, and its justification, will also better allow the investigation to be auditable if queries arise in the future.

A number of factors will affect the scope of the investigation. A narrow scope can help to focus resources and reach a quicker conclusion, but it may risk missing informative context. A wider scope can help to demonstrate that the investigation has been comprehensive, but it will increase the costs and time of the investigation. The appropriate scope will be affected by the nature of the issues (including whether the company is facing the risk of criminal, regulatory or civil action), the time pressures (especially if the company is in a race against co-infringers to apply for leniency) and whether there are, or are likely to be, concurrent investigations by authorities.

Defining the scope will also include deciding what the final deliverables will be. In some cases the default – a written report of factual findings – will be considered necessary, even though there is a risk that it may not be privileged. For example, in certain circumstances it may be advantageous to provide a written report to the authorities. The FCA Handbook states that a firm's willingness to volunteer the results of its own investigation, whether protected by legal privilege or otherwise, is welcomed by the FCA and is something the FCA may take into account when deciding what action to take.[18] Likewise, the DPA Code notes that co-operation (which is a public interest factor against prosecution) includes a company sharing its internal investigation report (including source documents) with the SFO; a point that has been highlighted by the courts in the DPA judgments handed down to date.[19] However, in other circumstances it may not be considered necessary or desirable to produce a potentially non-privileged written report. An alternative is for the investigation team to provide only oral updates on the factual findings. Other deliverables may include legal advice as to the company's exposure to litigation or investigation risk, self-reporting, employment law advice on disciplinary action against implicated employees, and mitigation and remediation proposals.

Companies must also assess whether to agree the scope of the internal investigation in advance with any authorities that are aware of the issue to be investigated. The benefits of doing so include potentially building co-operation

18 FCA Handbook, EG 3.11.2.

19 Deferred Prosecution Agreements Code of Practice, para. 2.8.2(i). Also see *Serious Fraud Office v. Rolls-Royce plc and Another* [2017] Lloyd's Rep FC 249, at para. 17; *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at para. 24; *Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435, at paras. 36 and 74; *Serious Fraud Office v. Güralp Systems Limited* [2020] Lloyd's Rep FC 90, at para. 27; S*erious Fraud Office v. Airline Services Limited* [2020] 10 WLUK 606, at para. 52; *Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep FC Plus 27, at para. 50.

credit with the authorities, reducing the risk of the authorities later criticising the scope of the investigation and allowing the authorities an opportunity to express their preferences as to the final deliverables and the conduct of the investigation. The SFO in particular has expressed concerns about the potential for internal investigations to 'trample over the crime scene', and early engagement can help to avoid later criticism of the investigation team's actions.[20] The FCA Handbook states that if a firm anticipates that it will disclose a report of its internal investigation to the FCA, the potential use and benefit to be derived from the report will be greater if the FCA has had the chance to comment on its proposed scope and purpose.[21]

Finally, at the scoping stage it can be helpful to assess what external resources may be required during the investigation, which could include forensic accountants, asset tracers, private investigators, public relations firms and foreign counsel.

5.6 Document preservation, collection and review

In any internal investigation, it is critical to consider as early as possible the practicalities for the preservation, collection, review and analysis of relevant material. In its Corporate Co-operation Guidance, the SFO states that co-operation includes preserving available evidence and producing it to the SFO in an 'evidentially sound' format.[22] Any decisions regarding data preservation and review should be recorded in writing to preserve a clear audit and 'chain of custody' trail.

Although in the early stages of an investigation it may not be appropriate to conduct formal interviews, the investigation team may wish to consider conducting informal 'scoping interviews' to assist with scoping the investigation and identifying where relevant material might be stored. Care should be taken, given the preference of a number of authorities that they be consulted prior to interviews (even those relating to the location of evidence) to avoid the possibility of criticism that the internal investigation might have tainted the recollection of witnesses.

5.6.1 Preservation

Document preservation is extremely important and must be addressed as early as possible. It can, in certain circumstances, be a criminal offence to destroy or dispose, or permit the destruction or disposal, of documents that may be relevant to an external investigation, and both the SFO and the FCA have brought prosecutions for such offences.[23]

---

20 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO (20 May 2015), available at https://www.sfo.gov.uk/2015/05/20/compliance-and-cooperation/.

21 FCA Handbook, EG 3.11.5.

22 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

23 Richard Kingston, Managing Director at Sweett Group plc, was convicted of offences contrary to s.2(16) Criminal Justice Act 1987 in December 2016, and in 2019–2020, the FCA brought a prosecution against Konstantin Vishnyak for offences under s.117(3) FSMA, of which Mr Vishnyak was acquitted at trial.

An important first step in document preservation is to identify which 'custodians' might hold information relevant to the investigation and which other sources might yield relevant documents (including any third-party sources). The sources of potentially relevant material may include emails, other electronic documents, external storage devices, mobile phones, tablets, internet messaging and chatroom data, telephone recordings[24] and hard copies. Companies should also identify any material they are unable to access (such as private email accounts, messaging applications or social media), as the relevant authorities may have statutory powers that allow them to access these sources. In its Corporate Co-operation Guidance, the SFO has stated it will consider it a mark of co-operation for companies to alert the SFO if there are any such inaccessible sources.[25]

The pool of custodians is likely to be broader than just those implicated in the suspected misconduct and may also include individuals reporting to them, individuals they reported to, secretaries and assistants, individuals in other departments they interacted with, and third parties outside the organisation. In some investigations, wider business units or offices might also be relevant.

In general, a company will issue a hold notice (also known as a document retention or document preservation notice) to such individuals asking them to preserve all (and not alter, discard, delete or destroy any) materials (including hard copies) they may hold relevant to the investigation. Beforehand, however, the company should consider whether circulation of the hold notice risks tipping off individuals relevant to the investigation who might destroy documentation or otherwise frustrate the investigation. In its Corporate Co-operation Guidance, the SFO states that genuine co-operation is inconsistent with 'putting subjects on notice and creating a danger of tampering with evidence or testimony'.[26] Potential solutions to address this risk include delaying the circulation of the hold notice until potentially relevant documentation has been secured or carefully drafting the hold notice so that it does not reveal the specific circumstances or subject matter of the investigation (subject, however, to the data privacy considerations discussed below). When drafting a hold notice a company should also consider the risk of it leaking and listed companies should consider whether the description in the hold notice is inside information.

Companies should take care to keep a clear record of the recipients of hold notices, especially where they are not circulated centrally, but instead are cascaded via the reporting structures of the organisation. As part of this, companies may wish to ask recipients to acknowledge their receipt and understanding of the hold notice, though this can create an administrative burden and raises the possibility that a recipient may refuse to acknowledge receipt. A middle ground may involve requesting an email read-receipt instead.

24 The FCA Handbook (SYSC 10A.1) places obligations on regulated firms to record telephone conversations that relate to regulated activities in certain financial instruments.

25 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

26 ibid.

In support of the hold notices (which are issued to, and place the burden of preservation on, the relevant individuals), companies should also consider what other steps they can take centrally to preserve relevant materials. This may include the suspension of regular document destruction processes, activating permanent email holds (preserving emails regardless of whether individuals delete emails from their inboxes), creating computer drive backups (so that if individuals delete data from a shared drive, it can be recovered), imaging custodians' devices and preventing the recall of hard-copy documents from archives without appropriate authorisation. As noted above, it is good practice to implement these before the circulation of the hold notice to reduce the risk of individuals deleting data.

Companies should also be alert to the possibility of relevant data being stored on legacy systems and take steps to ensure that such data remains accessible during the investigation.

When issuing hold notices or taking other steps to preserve relevant materials, companies should carefully consider the potential application of data privacy rules and appropriately document their consideration of data subjects' interests. Key considerations under Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR)) will include identifying a lawful basis under the GDPR for the preservation, ensuring appropriate transparency (so that, subject to certain exceptions, the data subjects are aware of the scope and purposes of the preservation), data minimisation (so that no more data is preserved than is necessary) and storage limitation (so that the data is not stored for longer than is necessary).

See Chapter 40 on data protection

5.6.2 Collection

Having preserved all potentially relevant materials, the next step is to identify what should be collected for review. This will usually be a smaller and more focused set of materials, and identifying them will involve assessing where the materials relevant to the investigation are most likely to be found, keeping in mind the scope of the investigation.

Depending on the circumstances of the investigation, it may be desirable to instruct an external forensic services provider to collect the data. This will be especially important in the criminal context where issues relating to the forensic integrity of the underlying data and chain of custody are key.

The company will need to consider whether to notify the affected individuals of the data collection. This will depend, among other things, on the terms of any applicable data privacy policies at the company and the likelihood that giving notice may result in individuals destroying documents or otherwise frustrating the investigation. In certain circumstances, express consent may be required from employees, especially if prescribed by data privacy laws or if the employees use their own devices.

See Chapter 40 on data protection

It will also be necessary to consider the application of data privacy rules to the collection more generally. In particular, requirements to minimise the data collected can require the use of date range and keyword search terms (even before the data is ingested into a review platform) and principle of integrity

and confidentiality may require the data to be stored securely and to be accessible only with appropriate authorisation.

Review 5.6.3

Having collected the data, in all but the smallest reviews, it is advisable to upload it to a document-review platform. This allows for easier searching, review and management of the data and will create an audit trail if questions arise in relation to specific documents.

The next stage will be to assess the appropriate searching criteria to help narrow the scope of the review and identify the most relevant documents. Available tools include applying date range, custodian and data source filters, and identifying relevant keyword search terms. If the timing allows, there are significant benefits to testing the potential searching criteria and refining them before starting the full review. There are also significant benefits to considering the appropriate type of data de-duplication to conduct.

Increasingly, vendors are offering technology-assisted analytics and technology-assisted review, in which the review software identifies links between documents or learns from initial reviewer coding decisions to identify similarly relevant documents from the remaining data set, so they can be brought to the attention of the review team sooner, or even automatically coded. The utility of this technology will, however, depend significantly on the quality of the initial 'seed set' of coding decisions and the complexity of the issues under review.

In any case, it is common to structure the review around a series of 'tiers', with an initial triage stage for relevancy, followed by second and potentially third-tier reviews by more senior individuals to focus the set and apply more complex coding. First-tier and even second-tier reviews are often outsourced to specialist document review service providers, which can free resource within the investigation team to concentrate on management of the review and other elements of the investigation.

To ensure accuracy and consistency of coding, it will be necessary to produce document review protocols and accompanying coding forms for each tier of the review, and to ensure the reviewers are fully briefed. It is also common to carry out regular quality control or calibration sessions with the reviewers, where they can ask questions of the senior team, and to set up a process for the rapid escalation to the senior team of key documents identified during the review.

In drafting the document review protocols and coding forms, it will be important to consider how the internal review may interact with any existing or potential parallel external investigation. In particular, if there is a possibility that relevant documents may be produced to an authority, there may be benefit in asking reviewers to code for privilege, data privacy, bank confidentiality and other jurisdiction-specific issues.

Documents located in multiple jurisdictions 5.6.4

Particular complexities can arise where documents, or other data, relevant to the internal investigation are located in other jurisdictions (including where

data is hosted on cloud-based or group-wide servers that might be physically located overseas).

It will often be necessary to get local data privacy advice before preserving and collecting data held overseas, including on whether and how the data may be transferred to the jurisdiction where the review is taking place. If transfer of the data is not permissible, it may be necessary to conduct a local review within the foreign jurisdiction.

There are also wider strategic considerations to bear in mind before deciding to collect and transfer data from other jurisdictions. In particular, consideration should be given to the risk of voluntarily transferring documents into a jurisdiction so that they become available to authorities or civil litigation counterparties when they might not otherwise have been available to those third parties (although this should be balanced against the risk that in not collecting this data the company may be found to be unco-operative or frustrating the investigation).[27] Further, where data is held by a subsidiary, it may be necessary for the subsidiary to enter into co-operation and information-sharing agreements with its parent in relation to the investigation. It is common in these agreements (especially where the subsidiary is not wholly owned) for the subsidiary to retain a right of consent prior to its data being disclosed to any authority.

5.6.5 Importance of record-keeping

It is critical at all stages of an internal investigation to keep clear records of key decisions taken, including the drafting of detailed, auditable summaries of the methodology undertaken for data preservation, collection and review. It will also be important to maintain full chain of custody records for any originals of relevant documents, as well as for devices.

The FCA Handbook states that where a firm conducts an internal investigation, it will be 'very helpful' if the firm maintains a proper record of the enquiries made and interviews conducted.[28] Likewise, in its Corporate Co-operation Guidance, the SFO has emphasised the importance of maintaining an audit trail of the acquisition and handling of digital, hard-copy and financial material, and the potential need for companies to identify a person to provide a witness statement covering such issues.[29]

---

27 It is possible for authorities in the United Kingdom to request documents from authorities in other jurisdictions via diplomatic channels, including via mutual legal assistance treaties. Further, criminal law enforcement agencies in the United Kingdom have the ability to seek electronic data held by communications service providers located in the United States under the Crime (Overseas Production Orders) Act 2019, which aims to simplify and speed up the process of obtaining electronic data located abroad. As to the limitations on the territorial scope of SFO notices under s.2(3) Criminal Justice Act 1987, see *R (on the application of KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2.

28 FCA Handbook, EG 3.11.9.

29 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

Appendix 1

About the Authors of Volume I

Jonathan Cotton
Slaughter and May

Jonathan Cotton is a partner in Slaughter and May's disputes and investigations group. He covers a range of cases involving contractual disputes, competition disputes and restructuring and insolvency matters. He also often advises on contentious aspects of corporate transactions, including takeovers.

He is particularly experienced in matters involving allegations of wrongdoing in its various forms. On the civil side, these have included cases involving the 'theft' of confidential information by employees and competitors, conspiracy and civil fraud. On the criminal and regulatory side, he has been involved in investigations and criminal prosecutions, cases concerning cartels, and regulatory cases concerning the UK Bribery Act, the Proceeds of Crime Act, the Fraud Act, Financial Services and Markets Act 2000, export controls and sanctions, and Companies Act offences.

The major investigations and disputes on which he has been engaged span business sectors including telecoms, investment banking, investment management, technology, heavy manufacturing, natural resources and fast-moving consumer goods.

Holly Ware
Slaughter and May

Holly Ware, a partner in Slaughter and May's disputes and investigations group, has a broad practice that includes litigation and contentious regulatory and criminal investigations.

She has cross-jurisdictional investigation experience involving both regulatory and prosecuting authorities, including the LIBOR investigations and others relating to bribery and corruption, market abuse, money laundering and data breaches.

Ella Williams

Slaughter and May

Ella Williams is senior counsel in Slaughter and May's disputes and investigations group. She has worked on some of the most complex, commercially sensitive multi-jurisdictional regulatory and criminal investigations of the past decade.

She advises corporations, financial institutions and individuals in relation to bribery and corruption, regulatory, tax and fraud investigations, including investigations and enforcement actions by the Financial Conduct Authority and Serious Fraud Office.

Slaughter and May

One Bunhill Row
London, EC1Y 8YY
United Kingdom
Tel: +44 20 7600 1200
Fax: +44 20 7090 5000
jonathan.cotton@slaughterandmay.com
holly.ware@slaughterandmay.com
ella.williams@slaughterandmay.com
www.slaughterandmay.com

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

ISBN 978-1-83862-272-5