Beginning an internal investigation: the UK perspective

Simon Airey, James Dobias and William Merry

1 Introduction

Whether, when and how to begin an internal company investigation are often decisions that must be made at speed, from a position of limited information and at a time when the business, and the individuals involved, may be under significant pressure or scrutiny. The following are a few of the key initial issues to address:

- how to determine what is in scope;
- how to conduct the document preservation, collection and review exercise;
- which individuals to interview and in what order;
- whether to involve external legal counsel;
- whether to notify any relevant authorities;
- how to structure governance and reporting; and
- how to maximise privilege.

Choices made at this early stage, or a failure to take into account the full context (including potential cross-jurisdictional issues), can have far-reaching repercussions. The focus of this chapter is to identify the key factors for companies to consider when grappling with these difficult issues.

2 Trigger points for internal investigations

The need for an investigation may arise from internal sources (e.g., routine monitoring, whistleblowing or internal audit findings), external sources (e.g., press reports, social media, customer complaints, external audit findings or litigation) or direct approaches from regulators or other authorities. Potential issues may also be uncovered during other internal or external investigations into other matters.

3 Whether to notify the authorities

A key question when an issue comes to light is whether there is an obligation to notify the relevant authorities or, if not, whether there may be a strategic benefit to doing so; and, if so, when.

This will turn partly on the regulatory status of the company or the individuals involved, the expectations of the relevant authorities and the size and nature of the issue itself. As different standards may apply to different authorities, especially across jurisdictions, it is often necessary to take a 'lowest common denominator' approach.

Firms regulated by the Financial Conduct Authority (FCA) are under a duty to deal with their regulator in an open and cooperative way and must disclose[1] appropriately 'anything relating to the firm' of which the FCA would reasonably expect notice.[2] While the FCA accepts that the timing of the notice will depend on the circumstances, it expects a firm to 'act reasonably' and discuss relevant matters with it 'at an early stage, before making any internal or external commitments'. In certain cases, the obligation to notify can be immediate.[3] Dual-regulated firms owe similar obligations to the Prudential Regulation Authority (PRA).[4]

Obligations to notify may also arise under applicable anti-money laundering and anti-terrorism rules. Persons working in the 'regulated sector' , as defined in the relevant legislation (e.g., the financial and real estate sectors, lawyers in relation to certain transactions, auditors, tax advisers, casinos and cryptoasset exchanges) must, subject to certain limited exceptions, submit a suspicious activity report (either directly or via their firm's nominated officer) to the National Crime Agency. This duty arises in relation to information that comes to them in the

1 See this guide's chapter on self-reporting to the authorities and other disclosure obligations from the UK perspective.

2 Financial Conduct Authority (FCA) Handbook, PRIN 2.1.1R, Principle 11. Relevant individuals may also be subject to equivalent rules under FCA Handbook, COCON 2.1.3R and COCON 2.2.4R. The FCA Handbook sets out a non-exhaustive list of situations where a firm is under an express duty to submit a notification, including where there has been a significant failure in the firm's systems or controls, a significant breach of a rule imposed by the FCA, employees may have committed a fraud against a customer, or a significant infringement of any applicable competition law has, or may have, occurred (FCA Handbook, SUP 15.3).

3 FCA Handbook, SUP 15.3 and SUP 15.7.11G.

4 Prudential Regulatory Authority (PRA) Rulebook, Notifications, Rule 2 and Fundamental Rule 7.

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.[5]

Even if a person does not work in the regulated sector, if they know or suspect that property they are dealing with constitutes or represents a person's benefit from criminal conduct, they are at risk of committing a money laundering offence unless they make an authorised disclosure and effectively receive 'consent' to continue with the activity (referred to as a defence against money laundering or DAML).[6]

Other notification requirements may arise under the rules of professional bodies,[7] the Charity Commission[8] or licensing authorities,[9] or under data privacy[10] or sanctions[11] legislation. Additionally, UK companies with substantial operations within the European Union may be required to include information about compliance-related matters in their financial reports. This could include

5 Proceeds of Crime Act 2002, ss.330 and 331 and Terrorism Act 2000, s.21A. The 'regulated sector' is defined in Schedule 9 to the Proceeds of Crime Act 2002 and Schedule 3A to the Terrorism Act 2000.

6 Proceeds of Crime Act 2002, ss.335, 338 and 340. Similar provisions apply in respect of terrorist financing (Terrorism Act 2000, s.21ZA).

7 For example, firms of solicitors are under an obligation to report certain matters to the Solicitors Regulation Authority (SRA), including any potentially serious breach of applicable regulatory requirements by themselves or another SRA-regulated person (SRA Code of Conduct for Firms, Rule 3), and accountants regulated by the Institute of Chartered Accountants in England and Wales (ICAEW) are under a duty to report any events that may indicate that a person regulated by the ICAEW may be liable to disciplinary action (ICAEW Disciplinary Bye-laws, 6.1).

8 Charity Commission, Guidance: 'How to report a serious incident in your charity', https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity.

9 For example, gambling operators licensed by the Gambling Commission of Great Britain are subject to notification obligations under the Licence Conditions and Codes of Practice (LCCP 15).

10 For example, data controllers are under a duty to notify the Information Commissioner's Office of personal data breaches 'without undue delay, and where feasible, not later than 72 hours after having become aware of it' (UK General Data Protection Regulation (GDPR), Article 33; Data Protection Act 2018, s.67).

11 Reporting obligations under UK sanctions laws vary depending on the relevant sanctions regime as enacted by the government using powers under the Sanctions and Anti-Money Laundering Act 2018; for example, Regulation 70 of The Russia (Sanctions) (EU Exit) Regulations 2019 requires certain firms and institutions to report to HM Treasury if they suspect that a person is designated or has committed an offence under those Regulations.

information relating to the number of convictions and the amount of fines received by the reporting company for violation of anti-corruption and anti-bribery laws, as well as information concerning actions taken by the company to address such breaches.[12]

Even where there is no obligation to notify the authorities, it may still be in a company's interests to make a voluntary disclosure; for example, while there is no obligation to notify the Serious Fraud Office (SFO) or HM Revenue & Customs (HMRC) of suspected criminal conduct, making a voluntary self-report to these bodies 'within a reasonable time of the offending coming to light' is listed as an example of cooperation[13] (which is a public interest factor tending against prosecution and in favour of resolution by way of a deferred prosecution agreement (DPA) or via an asset recovery power).[14] This reference to 'reasonable time' allows scope for a company to conduct at least a preliminary investigation into a potential issue prior to self-reporting. This was expressly acknowledged in a speech given in 2019 by the then Director of the SFO, who stated 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'.[15] In fact, the DPA Code of Practice specifically identifies 'reporting the wrongdoing but failing to verify it, or reporting it knowing or believing it to be inaccurate, misleading or incomplete' as a public interest factor in favour of prosecution (and against the granting of a DPA).[16] As such, appropriate diligence must be exercised when making a voluntary disclosure.

---

12 Directive (EU) 2022/2464, known as the Corporate Sustainability Reporting Directive, requires, *inter alia*, certain undertakings to include sustainability-related information in their financial reports, in line with the European Sustainability Reporting Standards (ESRS). ESRS G1 contains the relevant requirements as regards business conduct.

13 See this guide's chapter on cooperating with the authorities from the UK perspective.

14 Deferred Prosecution Agreements Code of Practice (DPA Code of Practice), para. 2.8.2(i). See also Serious Fraud Office (SFO), Corporate Co-operation Guidance, which states that cooperation includes 'identifying suspected wrong-doing and criminal conduct . . . [and] reporting this to the SFO within a reasonable time of the suspicions coming to light', and Corporate Self-Reporting Guidance, which states '[i]n appropriate cases the SFO may use its powers under proceeds of crime legislation [i.e., its asset recovery powers] as an alternative (or in addition) to prosecution'. Voluntary self-reporting has been viewed as an important public interest factor in the DPA judgments handed down to date, though it is not essential and several recent DPAs were not a product of voluntary disclosure.

15 Speech by Lisa Osofsky, then Director of the SFO, 'Fighting fraud and corruption in a shrinking world', 3 Apr. 2019, www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world.

16 DPA Code of Practice, para. 2.8.1(vi).

Balanced against this are the risks of a self-report, including that it may bring issues to the attention of the authorities that they might otherwise never become aware of, and that the scope of the authorities' focus may widen beyond the initial disclosure. A self-report that results in public censure or adverse publicity may also set in motion a number of related consequences, in addition to the costs, disruption and anguish often associated with dealing with the authorities. However, companies choosing to deal with the matter privately ought to bear in mind the risk that, should the issue later come to the attention of the authorities, negative inferences may be drawn (e.g., that the decision not to make a self-report was a cover-up).

Companies will also need to consider whether they are obliged to make any market disclosures. For companies with shares listed on relevant exchanges, including the Main Market or AIM, a duty to notify may arise if the fact of the underlying conduct, the contact with law enforcement authorities or the findings of the internal investigation constitute inside information, in which case the issuer should inform the public as soon as possible unless one of the specified grounds for delaying disclosure applies.[17]

4 Whether and when to launch an internal investigation

Deciding whether to launch an internal investigation is not always straightforward, and the risks and rewards should be balanced carefully. Once commenced, an investigation can develop in unexpected directions, consume considerable resources and be difficult to stop or limit without creating adverse inferences.

However, there are often a number of advantages to conducting an internal investigation, including the ability to gain a better understanding of the facts and legal exposures, which in turn may allow for more informed decision-making, the exploration of possible defences and placing the company in a proactive, rather than a reactive, position. There can also be significant benefits if the investigation disposes of damaging allegations, removes the risk of litigation or an investigation by the authorities, restores reputation or eliminates the need for a provision in the company accounts.

An internal investigation may also result in significant financial benefits if it allows the company to self-report and cooperate with an external investigation (avoiding the damaging effects of a prosecution and obtaining a discount on

17 EU Market Abuse Regulation (as retained under UK law), Article 17; European Securities and Markets Authority, 'MAR Guidelines: Delay in the disclosure of inside information and interactions with prudential supervision'; FCA Handbook, DTR 2.5.

any financial penalty); and a company may even be able to apply for leniency or complete immunity (principally in the sphere of competition and antitrust law). The findings of an internal investigation can also form the basis for more effective remediation to help avoid the conduct occurring again and can help to demonstrate that a company has appropriate procedures in place, a corporate culture that takes compliance seriously and effective disciplinary measures.

Increasingly, auditors may demand reassurance on issues before signing off on the company accounts or supporting a company with an initial public offering. The new Labour government in the United Kingdom has announced plans to enact major reform to the regulation of auditors, including the introduction of a new regulator (the Audit, Reporting and Governance Authority) with enhanced powers of oversight.[18] Although the extent of the new regulator's powers remains to be seen, it could be that a by-product of this increased scrutiny is that auditors will require further comfort from their clients regarding compliance-related matters before they will sign off accounts. Bankers, insurers and independent directors may also demand appropriate comfort, as might investors, potential acquirers or joint venture partners as part of increasingly focused due diligence. In this regard, investigations can be deployed positively and strategically rather than merely defensively or in negative circumstances.

In certain cases, there may be a specific requirement to undertake an internal investigation, whether by reason of applicable regulatory obligations,[19] directors' duties[20] or contractual obligations, or pursuant to existing policies and procedures. Likewise, an investigation may be required before renewing insurance to provide the required declarations.

On the other hand, internal investigations often have high costs and can be resource intensive, distracting management from 'business as usual' operations. There is also the risk of 'mission creep', whereby the focus of an investigation can widen in unexpected directions with attendant increases in disruption and expense. Depending on the context, it may also be strategically preferable to delay investigating an issue so as not to taint management with knowledge of wrongdoing at a particularly sensitive time for the business and to avoid making premature disclosures or notifications to various stakeholders (e.g., insurers,

18 The King's Speech 2024, 17 July 2024, https://www.gov.uk/government/speeches/the-kings-speech-2024.

19 For example, an FCA-authorised firm may consider an investigation is required to comply with its duty to conduct its business with integrity, due skill, care and diligence (FCA Handbook, PRIN 2.1.1R).

20 Companies Act 2006, ss.171 to 177.

auditors, lenders, clients and customers). There is also the risk that a hasty or poorly constructed investigation could lead to the creation of non-privileged documents that could assist regulators, prosecutors or opponents in civil litigation, especially if communications are careless, ambiguous or incriminating. If sufficient care is not taken, the dissemination of otherwise confidential information can also result in an inadvertent loss of legal privilege.

In certain cases, relevant authorities have been known to request that companies do not conduct an internal investigation or speak to potential witnesses, or to delay doing so. The FCA has stated '[w]hether 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', giving the example of where the FCA suspects that an insider dealing ring may be operating (whereby, if the firm were to conduct an internal investigation, this could prejudice the FCA's monitoring of the suspects).[21] The SFO has made similar observations.

5 Whether to instruct external legal counsel

Companies will need to consider at an early stage whether to instruct external legal counsel. While running an investigation in-house can be suitable for smaller and less complex investigations and can often result in notable cost savings, the involvement of external counsel can provide additional comfort and expertise, help bolster the independence of the investigation and provide an external viewpoint to balance the views and objectives of internal stakeholders. In this regard, the recently published UK government guidance in respect of the new 'failure to prevent fraud' offence under section 199 of the Economic Crime and Corporate Transparency Act 2023 states that internal investigations should be 'independent, clear about their internal client and purpose, appropriately resourced, empowered and scoped (including through legal advice), and legally compliant'.[22]

Using external counsel also helps increase the likelihood that privilege may apply to investigation documents, especially where in-house counsel hold dual business and legal functions or the privilege rules of certain other jurisdictions may be relevant (which jurisdictions may not recognise in-house counsel

21 FCA Handbook, EG 3.11.7. Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence) FCA, 'Internal investigations by firms', 5 Nov. 2015, www.fca.org.uk/news/speeches/internal-investigations-firms.

22 'Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud', published by the UK Home Office in November 2024.

communications as being privileged). To help ensure independence and avoid potential conflicts, the company may wish to use different external counsel from their normal corporate or transactional counsel.

6 Oversight and management of the investigation

Once the decision has been taken to undertake an internal investigation, it will be necessary to put in place an appropriate governance structure and reporting framework.

Day-to-day management of an investigation is often given to the internal legal or compliance teams, who will be the primary points of contact for external legal counsel and likely, therefore, the 'client' for the purposes of giving instructions and receiving legal advice (relevant to the question of when legal advice and litigation privilege may arise[23]). One of the issues for the Court of Appeal in the landmark case of *Al Sadeq v. Dechert* was whether legal advice privilege could apply to materials generated by external lawyers as part of an investigation they had been instructed to undertake. The Court noted that 'legal expertise extends not only to advice on black letter law and its application to particular facts, but also to the practical aspects of legal proceedings and preparations therefor' and concluded that investigatory work undertaken in a legal context can attract legal advice privilege.[24] That said, the case law concerning privilege in an investigatory context is complex and the question of whether any document generated as part of an investigation attracts privilege remains a fact-specific issue.[25]

In any event, it is important that potentially implicated individuals are excluded from the investigation team, whose membership should be kept under review as additional information is uncovered. If external legal counsel have been instructed to conduct an independent review, to preserve independence, it may be necessary to limit the ability of the client to instruct or influence the review beyond clearly defined parameters.

Whom the investigation team will report to will be determined partly by a company's existing corporate governance structure, though it is common for reporting to be made to the board or to the audit committee. In certain cases, it can be effective to constitute a specialised review body (e.g., a subcommittee of the board or a panel of senior employees and external advisers) and, in such

23 See this guide's chapter on privilege from the UK perspective.

24 *Al Sadeq v. Dechert LLP & Ors* [2024] EWCA Civ 28 at [229].

25 Note, for example, that the respondent law firm in *Al Sadeq v. Dechert LLP* accepted that documents created by lawyers as part of a 'purely investigative role', divorced from the firm's role as lawyers, would not attract privilege (at [230]).

circumstances, it will be necessary to specify clear terms of reference with delegated authorities and appropriate confidentiality protocols. Where the allegations involve subsidiaries, considerations of corporate separateness may require separate reporting into their own management.

It will also be helpful at this initial stage to consider the position of any whistleblowers and, in particular, the balance between providing them with comfort as to their position and receiving the information required to progress the investigation. While offering anonymity or confidentiality can put whistleblowers at ease, it can make it difficult to gather additional information and limit required internal and external reporting. There is also the question of whether the whistleblower is to be kept updated on the status and outcome of the investigation, recognising that communications with them may not necessarily be protected by privilege.

7 Scoping the investigation

Having a clearly defined scope, often supported by written terms of reference and an investigation plan, can help ensure that the objectives of the investigation are clear and avoid a wider-ranging unfocused exercise. Choosing a narrow scope can help focus resources and reach a speedier conclusion, although it can risk missing potential issues or relevant context, or result in the scope needing to be widened at a later stage (with the consequent potential delay and duplication of work). A wider scope can help to demonstrate that the investigation has been comprehensive but may increase the costs and length of the investigation; it may also result in unnecessary disruption to the business, or bring to light separate issues that may prolong or complicate the original investigation.

The scope will also be affected by the nature of the issues, the expectations of any authorities and the applicable time pressures (e.g., if a frustrated whistleblower is involved, leaks to the media have occurred, a relevant financial reporting deadline is looming, or the company is in a race with co-infringers for leniency).

One of the key decisions to be made as part of the scoping exercise is to define the final deliverables. This will often include a written report of the factual findings, but care should be taken to consider whether this will be privileged in all

relevant jurisdictions, or at all. The company may also decide to prepare a written report to the authorities, alongside certain underlying materials (such as notes of interviews).[26]

The DPA Code of Practice identifies providing a report in respect of any internal investigation plus source documents as an example of cooperation, and the FCA Handbook notes that sharing the outcome of an investigation is welcomed by the FCA and may be taken into account when deciding what action it will take, if any.[27] In disclosing such reports and other materials to the authorities, companies may seek protections as to how the information may be used or to whom it may be disclosed (e.g., via confidentiality restrictions or a limited waiver of privilege); however, these terms may not be acceptable to the authorities, especially if they are concerned about disclosure obligations in future individual prosecutions.

Decisions by companies to waive privilege voluntarily (even if on a limited basis) and to make material available to the regulators without requiring the use of powers of compulsion have been deemed an example of 'genuine and proactive' cooperation in a number of cases.[28] However, it is also important to consider potential cross-jurisdictional issues, as a limited waiver in one jurisdiction may amount to full waiver in another.[29] An alternative in this situation may be to provide only oral updates to the authorities or to allow them to view a report and related materials but not take a copy, though this will not always be acceptable. Other deliverables can include providing legal advice on the company's exposure, the merits of self-reporting and the employment position of implicated individuals, together with proposals as to mitigation and remediation.

---

26 The FCA's position is that if a firm decides to give a report to the FCA, 'the greatest mutual benefit is most likely to flow from disclosure of the report itself and any supporting papers. A reluctance to disclose these source materials will, in the FCA's opinion, devalue the usefulness of the report and may require the FCA to undertake additional enquiries' (FCA Handbook, EG 3.11.11).

27 DPA Code of Practice, para. 2.8.2(i); FCA Handbook, EG 3.11.2. Voluntary production of investigation reports has been viewed as an important public interest factor in the DPA judgments handed down to date.

28 See *Serious Fraud Office v. Airline Services Limited* [2020] at [51(b)] and [72]; and *Serious Fraud Office v. (1) Bluu Solutions Limited and (2) Tetris-Projects Limited* [2023] EWHC 1976 (KB), at [72(13)].

29 FCA Handbook, EG 3.11.13 ('the FCA cannot accept any condition or stipulation which would purport to restrict its ability to use the information in the exercise of the FCA's statutory functions. In this sense, the FCA cannot "close its eyes" to information received').

Companies may also need to consider whether to seek to agree the scope of the proposed investigation with relevant authorities up front. Doing so can build cooperation credit, reduce the risk of later criticism and allow the authorities the opportunity to express preferences regarding the final deliverables. The FCA has noted that, while it will not necessarily want to be involved in discussing the scope of a report in every situation, the potential use and benefit to be derived from the report will be greater if it has had the chance to comment on its proposed scope and purpose.[30] The SFO has also expressed concern about the potential for internal investigations to 'trample over the crime scene' and involving it in early scoping discussions can help forestall such criticism at a later stage.[31]

This early dialogue with authorities can also be used to agree the timing and format of witness interviews, which are often an area of dispute later (especially with regard to privilege).[32]

Companies will also wish to consider the external resources that may be required, including local and foreign counsel, forensic accountants, asset tracers, private investigators, translators, subject-matter experts and public relations firms.

8 Document preservation, collection and review

Core to any internal investigation will be the preservation, collection and review of relevant materials. In its Corporate Co-operation Guidance, the SFO states that cooperation includes 'preserving available evidence and providing it promptly in an evidentially sound format'.

While in the early stages of an investigation it may be premature to conduct formal interviews, it may be helpful to conduct informal scoping interviews to assist with understanding the issues involved and identifying where relevant material

30 FCA Handbook, EG 3.11.5.

31 Speech by Ben Morgan, then Joint Head of Bribery and Corruption SFO, 'Compliance and cooperation', 20 May 2015, www.sfo.gov.uk/2015/05/20/compliance-and-cooperation. The SFO states in its Corporate Co-operation Guidance that cooperation includes avoiding prejudice to an investigation by consulting 'in a timely way with the SFO before interviewing potential witnesses or suspects, taking personnel/HR actions or taking other overt steps'.

32 The FCA has noted: 'A practice we sometimes see is for the investigation to produce only lawyers' notes of such interviews. No recordings, no notes by others including the interviewee. Then firms will sometimes argue that the notes of the interview are privileged. This sort of approach looks to us like a "gaming" of the process in order to shroud the output of an investigation in privilege. We find it particularly unhelpful and unwelcome' (speech by Jamie Symington, supra note 21).

might be stored. This should be balanced against the preference of a number of authorities that they be consulted prior to interviews to avoid the possibility that the investigation may 'taint the recollection' of potential witnesses.[33]

8.1 Preservation

Ensuring that relevant documents are preserved is of critical importance and should be addressed as early as possible. Not only will failing to preserve relevant documents hamper the investigation but it can also, in certain cases, be a criminal offence to permit the destruction or disposal of relevant documents, with both the SFO and the FCA having brought prosecutions in this regard.[34]

The first step will be to identify which sources of data might be available (which can include emails, other electronic documents, external storage devices, mobile phones, decommissioned computer equipment, legacy systems, messaging and chatroom data, financial data, social media, video files, audio recordings[35] and hard copies), the location of this data, and who the relevant custodians might be (i.e., the individuals whose data may be relevant to the issues under investigation). With an increase in homeworking and the use of personal devices, companies should also consider what equipment, documents or information have been taken or are stored off-site.

The list of potential custodians will often be significantly broader than those implicated in the suspected misconduct and may include other team members, reports, assistants and those with whom they interacted in other parts of the organisation. It is worthwhile keeping a list of materials that cannot be accessed

33 The SFO Corporate Co-operation Guidance states that cooperation includes refraining 'from tainting a potential witness's recollection, for example, by sharing or inviting comment on another person's account or showing the witness documents that they have not previously seen'.

34 In December 2016, Richard Kingston, Managing Director at Sweett Group plc, was convicted of concealing, destroying or otherwise disposing of two mobile telephones (contrary to s.2(16) of the Criminal Justice Act 1987), and from 2019 to 2020, the FCA brought a prosecution against Konstantin Vishnyak for falsifying, concealing, destroying or otherwise disposing of a document that he knew or suspected to be relevant to the investigation (contrary to s.177(3)(a) of the Financial Services and Markets Act 2000), though Mr Vishnyak was acquitted at trial.

35 FCA Handbook, SYSC 10A.1R requires FCA-regulated firms to record telephone conversations that relate to regulated activities in specified financial instruments.

(e.g., private email accounts, bring-your-own electronic devices or third-party bank account information) as the authorities may have statutory powers that allow them to access these sources.[36]

Many organisations will issue a hold notice (also known as a document retention or document preservation notice) to relevant custodians, instructing them to preserve all relevant documents in their possession and control. This should be balanced against the risk of tipping off individuals as to the fact of the investigation, potentially providing them with an opportunity to destroy relevant evidence.

In its Corporate Co-operation Guidance, the SFO states that genuine cooperation is inconsistent with 'putting subjects on notice and creating a danger of tampering with evidence or testimony'. Potential solutions in this regard can include delaying the circulation of the hold notice until known sources of documents have been secured, or carefully drafting the hold notice so that it does not reveal sufficient details about the investigation to put individuals on notice (although this will need to be balanced against the data privacy requirements outlined below). Consideration may also need to be given to the risk that the hold notice is leaked and, if so, whether it might contain inside information that has not yet been disclosed to the market or may result in damaging media reporting or speculation. A clear record should be kept of the recipients of the hold notice.

In support of a hold notice, companies should consider whether to implement other steps centrally to preserve relevant materials. This can include the activation of permanent email holds (which prevent individuals from being able to delete their emails permanently), the suspension of regular document destruction processes, creating computer drive backups, imaging devices such as laptops and mobile phones (which can be especially important if relevant custodians are leaving the organisation and those devices would otherwise be wiped), retaining user access logs and preventing the recall of hard-copy documents from archives. It can often be good practice to put these processes in place prior to the circulation of the hold notice to reduce the potential for individuals to seek to tamper with potentially relevant materials.

Steps should also be taken to maintain access to legacy systems and software (e.g., by renewing user licences) and more generally to ensure that data being preserved can still be accessed.

---

36 For example, the SFO's powers under the Criminal Justice Act 1987, s.2(3). Alerting the SFO to inaccessible materials is listed as an example of cooperation in the SFO Corporate Co-operation Guidance.

When undertaking these steps, companies should give careful consideration to the requirements of applicable data privacy legislation and appropriately document their consideration of the protection of data subjects' interests. Key considerations under the General Data Protection Regulation as retained under UK law (UK GDPR[37]) include identifying a lawful basis for preservation, ensuring appropriate transparency (so that 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 data is not stored for longer than is necessary).[38]

8.2 Collection

Having preserved potentially relevant materials, the next step is to identify the data to be collected for review. This will usually be a smaller set of materials, enabling a more focused review and cost savings (as many document review platforms charge monthly fees per gigabyte of data being hosted).

In certain cases, it may be desirable to instruct an external forensic services provider to collect and process the data, especially in the criminal context where the forensic integrity of data and 'chain of custody' records are key.

The investigation team will need to consider whether to notify affected individuals of the collection, which will turn partly on the applicable data privacy laws, the scope of any privacy notices in place and any tipping-off risk. In certain circumstances, express consent to the collection of data may be required from the individuals (e.g., under applicable data privacy laws or if the company wishes to image the employees' personal devices).

8.3 Review

In all but the smallest reviews, it is advisable to upload the data collected to a document review platform, which allows for easier searching, review and management of the data and related metadata, and creates a reliable audit trail.

It will then be necessary to decide on appropriate searching criteria, which can include running filters (e.g., as to date range, custodian and data source) and key word search terms. De-duplicating the data can help reduce hit counts and ensure a speedier review.

37 https://www.legislation.gov.uk/eur/2016/679/contents.

38 UK GDPR, Article 5.

Increasingly, document review platforms are offering technology-assisted review and technology-assisted analytics (at times supported by artificial intelligence), under which the review software can identify links between documents or learn from initial reviewer coding decisions to identify relevant documents. These documents can then be prioritised for manual review (helping to ensure that relevant documents are identified more quickly) or even automatically coded as relevant or not relevant. The utility of this software can turn, however, on the quality of the 'seed set' of documents and the complexity of the issues, meaning it is important to conduct robust quality control checks.

It is common to structure the review itself around tiers, with the first tier focusing on an initial triage for relevance and the second or third tiers being undertaken by more senior individuals applying more complex coding. In certain cases, there can be resource savings through outsourcing the initial tiers of the review to specialist external document review service providers.

To help ensure consistency and quality in the review, document review protocols and coding forms may be created for each tier, combined with briefings on the issues and regular quality control or 'calibration' sessions and dip tests. It is also helpful to put in place processes for the rapid escalation to the senior team of particularly relevant documents.

As the review can often be the most expensive and resource-intensive stage of an investigation, it can be tempting to seek to address as many points as possible in one coding form; however, this should be balanced against the risk of overburdening reviewers, which may not only slow down the review but also lead to lower-quality results or even errors or omissions.

If various parties are to share a document review platform (such as the company and employees with separate legal representation), it is important to ensure a clear separation of access rights, otherwise there is the risk that one party's sensitive work-product may be visible to another party.

8.4 Documents located in other jurisdictions

Particular complexities can arise where documents or other data that are relevant to the investigation are located in other jurisdictions (including being hosted on cloud-based or group-wide servers physically located overseas). In such cases, it will often be necessary to get local law advice as to whether this data may be transferred to the jurisdiction of review. If such a transfer is not permissible, it may be necessary to conduct the review overseas.

There are also wider strategic risks associated with voluntarily transferring documents into a specific jurisdiction. Consideration should be given to whether this may make such documents available to regulatory or law enforcement

authorities or to opponents in civil litigation where they might not otherwise have been (although this should be balanced against the risk that not doing so may appear uncooperative or even obstructive).

The SFO is unable to use its powers under section 2(3) of the Criminal Justice Act 1987 to compel a foreign company to produce data it holds outside the United Kingdom; however, it can compel companies incorporated, and individuals located, in the United Kingdom to transfer data into the country if they have possession or control over it (e.g., if the UK parent can direct the decisions of a foreign subsidiary).[39] Even where a company does not voluntarily transfer data into the United Kingdom, domestic authorities may request documents from authorities in other jurisdictions, including via mutual legal assistance channels or the UK–US Data Access Agreement, which allows law enforcement authorities in the United Kingdom and the United States to request data held by telecommunications providers in each other's jurisdictions without the need for a mutual legal assistance agreement.[40]

8.5 Record-keeping

It is important to keep clear records of all key decisions taken throughout an internal investigation, together with a full audit trail and chain of custody for the document preservation, collection and review process.

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.[41] 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 material and devices, and hard-copy and financial material, and the potential need for companies to identify a person to provide a witness statement covering such issues.

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

40 See https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet/policy-factsheet-on-the-uk-us-data-access-agreement.

41 FCA Handbook, EG 3.11.9.

Contact details & biographies

McDermott Will & Emery UK LLP

22 Bishopsgate
London, EC2N 4BQ
United Kingdom
Tel: +44 20 7577 6900
sairey@mwe.com
jdobias@mwe.com
wmerry@mwe.com
www.mwe.com

Firm description
https://www.mwe.com/about/

Simon Airey

McDermott Will & Emery UK LLP

Simon Airey is the global co-head of investigations and compliance at McDermott Will & Emery in London and focuses his practice on global, cross-border and internal investigations, financial and regulatory crime, bribery and corruption, money laundering, tax and fraud inquiries, data breaches, dawn raids, asset tracing, international enforcement and corporate compliance issues.

He has conducted a wide range of investigations and corporate defence assignments in different sectors, including construction, defence, financial services, gambling, oil and gas, logistics, pharmaceuticals and telecommunications. Simon represents both companies and individuals in criminal and regulatory proceedings and in associated litigation by agencies such as the Serious Fraud Office, the Crown Prosecution Service, the Financial Conduct Authority and HM Revenue & Customs.

Simon advises a large number of multinational groups on their global compliance programmes and assists clients with corporate risk assessments and M&A due diligence. He conducts tailored training for boards and senior management and has lectured around the world on a range of topics, including the UK Bribery Act, the UK Criminal Finances Act and the Economic Crime and Corporate Transparency Act 2023. He advises a number of organisations on the corporate criminal offence of failure to prevent the facilitation of tax evasion and served on the Law Society committee that devised related guidance for the legal profession.
https://www.mwe.com/people/simon-airey/

James Dobias
McDermott Will & Emery UK LLP

James Dobias's practice covers a wide range of domestic and international corporate crime and investigations-related matters, including bribery, corruption, money laundering, tax evasion, fraud, data breach and associated regulatory and compliance issues.

He has experience assisting with and advising on internal investigations, investigations conducted by the Serious Fraud Office, Crown Prosecution Service, Financial Conduct Authority, Takeover Panel, HM Revenue & Customs and professional regulators, anti-bribery and corruption compliance, whistleblowing, anti-money laundering issues and risk assessments. James has also developed a particular expertise on deferred prosecution agreements (DPAs), having advised on two of the largest and most complex DPAs in UK legal history (each for FTSE 100 companies).

Prior to joining McDermott, James trained, qualified and spent the majority of his career at an international law firm, during which he worked on some of the highest profile and most complex cases in the corporate crime sphere and was seconded to a FTSE 100 company to work on its ongoing SFO investigation. James has also worked for a litigation funder, where he specialised in overseeing group litigation and class actions arising out of regulatory issues.
https://www.mwe.com/people/james-dobias/

William Merry
McDermott Will & Emery UK LLP

William Merry has a practice covering a range of domestic and international corporate crime and investigations-related matters. He has experience in resolving anti-bribery and corruption, anti-money laundering, fraud, blackmail and sanctions matters in both contentious and non-contentious contexts. This expertise extends to dealing with investigations or prosecutions brought by the Serious Fraud Office, the Financial Conduct Authority, HM Revenue & Customs, the Crown Prosecution Service, the National Crime Agency, Companies House and others, as well as the conduct of internal compliance investigations. He has most recently advised on the second-largest deferred prosecution agreement in UK legal history.

William has developed particular expertise on UK sanctions laws following Russia's invasion of Ukraine. Additionally, he has provided a range of advice and training to multinational corporates in respect of the United Kingdom's new

Economic Crime and Corporate Transparency Act 2023 (including, in particular, in respect of the new senior manager regime for corporate criminal liability and the failure to prevent fraud offence).

Prior to joining McDermott, William gained experience at an international law firm, during which time he spent periods on secondment to two major financial institutions. He also has experience of acting on contentious property and employment law-related disputes for pro bono clients. Aside from his fee-earning work, William is a trustee of a mental health charity and co-leads on McDermott's wellbeing programme in London.
https://www.mwe.com/people/william-merry/