6

Beginning an Internal Investigation: The US Perspective

Bruce E Yannett and David Sarratt[1]

6.1 Introduction

The aim of this chapter is to provide the reader with useful tools to navigate the beginning of an internal investigation. Mistakes made in the initial phases of an investigation can have costly repercussions down the road, and, for this reason, it is important to consider all the relevant legal, commercial and logistical factors in making strategic decisions early on.

6.2 Assessing if an internal investigation is necessary

Information giving rise to the need for an internal investigation can come from a variety of sources, including customers, employees, whistleblowers, lawsuits, counterparties, news and social media, as well as from prosecutorial and regulatory authorities. Regulatory changes have created new incentives for individuals to come forward and report suspected wrongdoing. For example, the Sarbanes-Oxley Act of 2002, and its implementing rules, require attorneys who appear and practise before the SEC to report evidence of a material violation up the ladder to a company's chief legal officer and CEO. The reporting obligation is not discharged until the attorney reasonably believes the company has provided an appropriate response.[2] Similar reporting obligations apply to issuers and auditors.[3]

When confronted with information – from whatever source – that the company or its employees may have engaged in serious misconduct, in-house counsel's first step is often to assess whether it would be in the company's interest to conduct an internal investigation. Counsel will want to consider whether

1 Bruce E Yannett and David Sarratt are partners at Debevoise & Plimpton LLP.

2 See Sarbanes-Oxley Act of 2002 § 307, 15 U.S.C.A. § 7245 (2002); 17 C.F.R. Part 205.3(d).

3 See Securities Exchange Act of 1934 § 10A, 15 U.S.C.A. § 78j-1.

government authorities are already investigating, or are likely to investigate, the matter, whether civil litigation will follow and in what form, and the potential (or likely) need for remediation. Depending on the facts, counsel may also want to balance the costs of investigating and the potential disruption to normal business, as well as any potential reputational risk or commercial fallout.

In some instances, external legal obligations may require an investigation to be conducted. Board members and management, for example, have a fiduciary duty to protect the interests of the corporation and its shareholders, and in some cases that duty will include an obligation to investigate indications of serious misconduct at the company. An investigation may also be required in certain instances so that company executives can meet any affirmative certification obligations they have, whether under Sarbanes-Oxley or otherwise.

More often, however, counsel will want to conduct an investigation to make an informed decision about whether it is in the company's interest to self-report the matter to law enforcement or regulators. Over the past two decades, the United States Department of Justice (DOJ) has placed an increasing focus on self-reporting both in charging decisions and in the degree of co-operation credit that will be afforded to a company. To guide the charging decisions of its own attorneys, the DOJ has set out a number of factors that prosecutors should consider in determining whether to charge a business entity, including co-operation and voluntary disclosure, the adequacy of the corporation's compliance programmes, and any remedial actions or restitution undertaken.[4] The DOJ has expanded on these factors through subsequent directives,[5] such as the Yates Memorandum of 2015, which made clear that 'in order to qualify for *any* co-operation credit, corporations must provide to the [DOJ] all relevant facts relating to the individuals responsible for the misconduct.' Additionally, in 2016, the Fraud Section of the DOJ launched a 'Pilot Program' announcing even greater emphasis on voluntary self-reporting in deciding whether to charge or how to resolve corporate criminal matters.[6] The following year, this policy was formally implemented through the DOJ's revised Policy on Corporate Enforcement of the Foreign Corrupt Practices

See Chapter 4 on self-reporting to the authorities

4 See Holder Memorandum, Bringing Criminal Charges Against Corporations, Dep't of Justice, Deputy Attorney General Eric Holder (16 June 1999).

5 See Thompson Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Larry D. Thompson (20 January 2003); McCallum Memorandum, Waiver of Corporate Attorney–client and Work Product Protections, Dep't of Justice, Acting Deputy Attorney General Robert D. McCallum (21 October 2005); McNulty Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Paul J. McNulty (12 December 2006); Filip Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Mark Filip (28 August 2008).

6 Yates Memorandum, Individual Accountability for Corporate Wrongdoing, Dep't of Justice, Deputy Attorney General Sally Q. Yates (9 September 2015) (emphasis added); Leslie R. Caldwell, Criminal Division Launches New FCPA Pilot Program (5 April 2016) (noting that '[i]f a company opts not to self-disclose, it should do so understanding that in any eventual investigation that decision will result in a significantly different outcome than if the company had voluntarily disclosed the conduct to us.').

Act, which was announced on 29 November 2017 and closely tracks the objectives of the Pilot Program, including the incentives for self-disclosure and co-operation with the DOJ's investigations.[7] The DOJ has since indicated that this policy will likely be extended, at least in practice, to cases that come before the Department involving other federal regulations beyond the FCPA.[8]

In light of these policies, for all practical purposes, an internal investigation is often necessary so that the company can identify what, if any, information should be disclosed to the DOJ, and whether co-operation credit is attainable. This, however, may be a false dilemma as, in many instances, a corporation's co-operation can be the most significant determining factor in how the DOJ resolves a case, including the amount of any penalty.[9]

Many regulatory agencies have likewise increasingly come to expect companies to perform a robust internal investigation of any potential legal or regulatory violations and to report such violations to the agency. For example, the Consumer Financial Protection Bureau (CFPB) has stated that 'responsible conduct' – namely proactive self-policing for potential violations, prompt self-reporting of identified violations, complete remediation of resulting harm and co-operation with the CFPB – would influence the CFPB's resolution of an enforcement investigation.[10] Similarly, the US Department of Treasury Office of Foreign Assets Control specifically provides companies with mitigation credit of 50 per cent off its base penalty amounts for voluntary disclosures and further mitigation for co-operation.[11]

Even apart from legal considerations, business and reputational concerns alone may provide grounds for conducting an internal investigation. Indeed, counsel will often need to have a baseline understanding of the underlying facts, and an informed sense of whether there is any substance to the allegations of misconduct, in order to make a reasonable assessment of the potential business and legal consequences and the need for corrective action. Commencing a thorough internal inquiry will often also be important to any related public relations efforts, and will be critical to maintaining the company's credibility with its customers, business partners and other affected individuals.[12]

---

7 See Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, U.S. Dep't of Justice (29 November 2017); United States Department of Justice, 'United States Attorneys' Manual' §9-47.120 (FCPA Corporate Enforcement Policy – USAM Insert).

8 See Head of the Criminal Division John Cronan and Chief of the Securities and Financial Fraud Unit Benjamin Singer Deliver Remarks at the ABA's 32nd Annual National Institute on White Collar Crime (1 March 2018); Letter Declining to Prosecute Barclays PLC (28 February 2018), stating 'The Department's decision to close its investigation of this matter is based on a number of factors, including . . . Barclay's timely, voluntary self-disclosure'.

9 U.S.S.G. § 8C2.5(g), cmt. 13 (2015).

10 CFPB Bulletin 2013-06, Responsible Business Conduct (25 June 2013).

11 31 C.F.R. Part 501, Economic Sanctions Enforcement Guidelines (9 November 2009).

12 In rare circumstances, some facts will be so clearly unlawful on their face – e.g., if an employee is providing clearly and materially false information to investors – that the company should consider notifying the relevant law enforcement or regulatory authorities even before conducting a complete

Identifying the client 6.3

Once the company decides to commence an internal investigation, the next step is to determine who will conduct the investigation and for what specific client within the organisation. In large organisations, particularly those with multiple subsidiaries across the globe, counsel should think strategically about how to structure the investigation: where to locate the attorney–client relationship, to whom the investigating attorneys should report, and who will be making key decisions as the investigation proceeds. In making these decisions, counsel should consider what relationships will best protect the integrity and confidentiality of the investigation, the location and custody of relevant documents, and the overall aims of the investigation over the short and long term.

In some circumstances, counsel may also want to consider whether the investigation should be conducted on behalf of the board (or its subcommittee), with counsel reporting to and directed by the board, rather than by management. In a shareholder derivative suit, having the board direct the investigation will be the norm, both because the conduct of management will often be at issue and so that the investigation will not be subject to the derivative-claim exception to the attorney–client privilege recognised in some jurisdictions. The board may also be best suited to lead an investigation when the allegations are particularly serious or could have serious consequences for the company, when the allegations concern the actions of senior management, or when reputational or other concerns require that the investigation be conducted independently of management. Making that decision in any particular case will depend heavily on the specific facts involved, the company's business and position in the marketplace, the relationship dynamics at the company and the overall goals of the investigation.

See Chapter 36 on privilege

Whatever decision is made, it is important that the company clearly document who the client is, and the reporting and oversight structure for the investigation.

Control of the investigation: in-house or external counsel 6.4

Although routine matters can often be handled by in-house counsel, an outside firm should ordinarily conduct the investigation where the potential misconduct could produce significant adverse legal or commercial consequences for the company. Though internal investigations can be expensive and time-consuming, these concerns often pale in comparison to the possible legal, financial and reputational risks faced by the company, as well as the need to demonstrate independence. Hiring external counsel allows for a clearer application of attorney–client privilege to the communications and work-product of the outside firm, especially where corporation counsel has both business and legal functions. Often, both commercial and legal concerns can precipitate an internal investigation, so using external

internal investigation, particularly where time is of the essence and, if appropriate, continue with the internal investigation in parallel.

counsel can decrease the risk of inadvertently waiving privilege.[13] External counsel also brings expertise, experience and resources to support the company in challenging situations that are unlikely to arise with much frequency at any particular company.

Depending on the circumstances, in-house counsel may want to consider using external counsel that is not the company's usual firm.[14] Bringing in a separate firm that is less familiar with the company's business, of course, will often involve additional time and expense. Whether this step is justified in a particular case will depend on the sensitivity and significance of the investigation, the level of management implicated in the conduct, the need for perceived independence of the investigation, and the attitude of potentially relevant regulators who may be assessing the quality and results of the investigation in considering whether the company deserves credit for co-operation.

6.5 Determining the scope of the investigation

The importance of clarifying the investigation's scope and purpose at the outset cannot be overstated. First, a well-defined and memorialised purpose can help establish the legitimacy of privilege claims over attorney–client communications and work-product produced in the course of the investigation; the claim to attorney–client privilege is likely to be much stronger if an independent investigation has been commenced or litigation is reasonably in contemplation.

See Chapter 36 on privilege

Additionally, defining the investigation's purpose can impose a welcome discipline and accountability on the investigators themselves. Corporate counsel are quite familiar with the tangents that can cause an investigation to become rudderless and wasteful. As explained below, a short period of preliminary investigation can often be helpful in defining a purpose and scope to the investigation that is reasonably clear and realistic, while identifying key uncertainties and inflection points to come.

6.5.1 Key documents and scoping interviews

Most investigations will begin with counsel's review of a handful of critical documents that are at the heart of the information triggering the need for the investigation. In many instances, the documents themselves, rather than individuals, may have alerted the company to alleged wrongdoing and precipitated the need for an investigation. In almost every case, however, conducting a small number of initial scoping interviews will be a useful way for the investigators to focus in quickly on the truly important material.

Identifying the most useful individuals to speak with in these scoping conversations can be delicate, as investigators seek to strike a balance between speaking

13 See, e.g., *United States v. Ruehle*, 583 F.3d 600, 606-12 (9th Cir. 2009) (statements made for the purpose of disclosure to outside auditors not privileged).

14 See *In re John Doe Corp.*, 675 F.2d 482, 491 (2d Cir. 1982) (recognising that when corporate counsel finds evidence of criminality protected under *Upjohn* 'the wiser course may be to hire counsel with no other connection to the corporation to conduct investigations').

with individuals who are knowledgeable about the issue at hand but who are sufficiently removed from the potential misconduct that they can safely be viewed as reliable in terms of setting the scope and maintaining the confidentiality of the investigation. Of course, interviewing an employee at an early stage, without the benefit of a complete set facts or documents, could result in incomplete information and the need for a further interview.

One logical place for external counsel to start is to thoroughly debrief the in-house legal team and, potentially, the individual or individuals who brought the issue to the attention of the organisation. These interviews can serve to identify key custodians, the nature and volume of relevant documents, the ways documents are stored, and who has access to them. If there is an obvious investigation target, interviewing that individual in the initial stages may be more efficient, but this must be weighed against other strategic considerations, including alerting the target to the focus of the investigation and compromising the investigation later on. The timing and structure of these initial discussions may also be influenced by external deadlines or other business considerations involved in the review.

Identifying necessary partners 6.5.2

Another early consideration for counsel is what outside investigative partners may be needed. These can range from technical subject-matter experts to local counsel in foreign jurisdictions to data processing and hosting services to forensic accountants. Counsel ordinarily will want to interview a number of firms in deciding which vendors to use, and the discussions can sometimes yield helpful insight into the size of the tasks ahead, likely costs, potential alternative strategies and timing. Engaging these third parties at the outset of the investigation – even if their work is not needed immediately – will often be valuable in defining the scope and methods of the investigation. As noted above, given the consideration of attorney–client privilege, generally external counsel will retain the third-party vendors on behalf of the company so that their work and work-product is undertaken on the instruction of external counsel in anticipation of litigation and thereby covered by privilege and attorney work-product protections.

Developing a work plan 6.5.3

Once the investigating attorney has identified the subject matter of the investigation (the who, what, when and where), the scope and the purpose of the investigation and a concrete plan for carrying it out should ordinarily be memorialised by external counsel in a written work plan. This type of memorandum allows for client input on the investigative process, gives in-house counsel clear expectations about how the investigation will progress, and provides investigating attorneys with a benchmark for strategic judgements as the investigation moves forward. It can also serve as a useful tool for dividing responsibilities among the investigating attorneys and tracking progress toward key investigative goals. Keep in mind that the work plan may be a document that the company decides to share with the criminal or regulatory authorities and should be drafted accordingly.

In building the work plan, counsel should consider the time frame and geographical range of the inquiry, as well as which entities of the company (e.g., subsidiaries, affiliates, departments) will be covered and, if applicable, the rationale for not covering other entities at this stage. The memorandum should clearly set forth the subject matter under investigation and, to the extent possible, (1) what company documents will be retrieved (and by whom), (2) how data will be processed (and by whom), and (3) how documents will be reviewed (and by whom). In collecting, reviewing and preserving documents, the investigating attorney should take into account any data privacy concerns that may arise.

See Section 6.6.2

Where possible, the work plan should list any interviews that have been or will be conducted, or at least the categories of people to be interviewed. To the extent there is a rationale for interviewing some individuals and not others, it should be stated. Likewise, if the involvement of other third parties, such as forensic accountants and industry experts, is foreseeable, the document should describe the scope of their expected engagement.

The work plan should also set a rough schedule for key deliverables in the investigation, and at least tentatively identify the form that the ultimate work-product will take. In particular, it is useful to know at the outset of an investigation whether the preparation of a written investigative report will be useful and in the company's interest, or whether an oral presentation of findings to management or the board would be preferable. A written report will most often be advisable when the company believes providing the report to a third party or to the public will be beneficial, whether for reputational, business or legal reasons. In most other cases, an oral report will often serve the client's interests just as well without creating a risk of inadvertent or compelled disclosure.

Finally, the work plan should be flexible. Although careful planning is always beneficial, investigations in the real world are not scripted affairs. The investigative team will have to adapt to new information and challenges as the investigation progresses, and the work plan should lay out a process for making those decisions – particularly in terms of who should be consulted and who should approve – before the investigative team moves in a new direction not contemplated by the plan.

Certain investigations may implicate the general counsel or other members of senior management in alleged misconduct. In that circumstance, the investigating attorneys should report to the board (or a designated member or committee of the board) or to a senior executive who has no involvement in the facts at issue and who does not report to any member of management whose conduct may be under review.

6.6 Document preservation, collection and review

6.6.1 Preservation

As soon as possible after learning of potential misconduct, the in-house attorney should implement a litigation hold and document preservation notice to prevent the intentional or inadvertent destruction of relevant documents and material. In fashioning the document retention policy, it is ordinarily advisable to err on the side of overbreadth, at least at the beginning when the extent of any potential

wrongdoing and the relevant actors are unknown. This is critical. Failure to successfully preserve relevant material could be viewed as a dereliction of the attorney's duties and, in some cases, as obstruction of justice.

In issuing preservation or 'hold' notices, the investigating attorneys should consider who should receive these notices (including the IT and records departments), what types of documents and data should be included, and how the investigation should be described. Where notices are sent to different jurisdictions, the investigating attorney may need to consider providing translations as well as addressing data privacy restrictions. The attorney implementing the litigation hold should record the distribution of notices and, where extra caution is warranted, have employees sign and return a copy of the notice or electronically acknowledge receipt so as to create a record. If the company has received a subpoena from law enforcement relating to the subject matter of the investigation, the subpoena will define the minimum universe of documents that require preservation, but counsel should consider whether additional material should be preserved for purposes of the internal investigation or otherwise.

See Section 6.7

The investigating attorneys should consult with the company's records management department to preserve any hard-copy files, including those stored off-site in archives. The investigating attorney should also instruct the IT department to suspend any normal data destruction practices and to create and maintain a list of the relevant sources of data. Such sources may include documents maintained on the company's servers and employees' hard drives, emails saved on exchange servers, data held on employees' home computers, and data saved on employees' work-issued mobile devices. To the greatest extent possible, the company should take steps on its own to preserve this electronic data rather than relying on individual employees to preserve their own documents. The company should also take steps to prevent individuals from destroying or altering potentially relevant data. In some cases the facts will warrant proactive data capturing steps, including forensic images of employee laptops or desktops. Document custodians should be designated as soon as the investigating attorneys reasonably believe such individuals may possess documents relevant to the investigation.

It bears mention that sometimes the document collection process itself can come under scrutiny, particularly if authorities come to believe that relevant (and potentially damaging) documents may have been destroyed. In some extreme cases, someone with first-hand knowledge of the investigation may be called to provide sworn testimony in a deposition or in court. Attorneys should plan and document the collection process with this worst-case scenario in mind, and make clear to their clients the importance of treating the collection process – sometimes viewed as a ministerial chore – with serious care and attention.

Collection 6.6.2

Once preservation measures have been implemented, the investigation can turn its attention to the collection of documents. Almost all investigations require judgement calls to be made on the scope of collected documents, including whether the investigation can be accomplished in whole or in part through collection within

the company or, instead, requires collection from third parties. Company policies (e.g., codes of conduct) and local employment law also may impose limitations on the collection process. If the investigation contemplates the collection of personal health information, counsel should ensure that all data collection comports with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In such circumstances, counsel should take appropriate measures to safeguard personal health data, including assessing whether entering into a business associate contract is appropriate.[15] By the same token, counsel should ensure that any other personally identifiable information (PII) collected as part of the investigation is similarly flagged during review and appropriately safeguarded.

For electronic data, the process of collecting data will often coincide with preserving it. Counsel should make sure that forensic copies of all relevant electronic data (including metadata) has been copied to a secure location, preferably with at least one backup maintained on a separate system. The data will then need to be loaded into a review platform for review. Evidence that has been collected in paper form will often be most easily reviewed by digitising it and loading it into the same review platform as the electronic documents that have been collected. The data vendor retained by the investigating counsel will provide the collection and hosting support to the company.

As with the preservation process, the steps taken in collecting documents should be recorded. In instances where requested documents cannot be located, the search efforts and results should also be documented.

6.6.3 Review

Regarding the review of the documents, the investigating attorneys should carefully consider how best to manage the volume and formatting of documents. Outside vendors are a useful resource for these matters, and consulting with them can often save time and money.

Where there is a large volume of documents to be searched, the key objective is to locate the responsive documents quickly and efficiently. Search terms should be broad enough to include responsive materials, but narrow enough not to bog down review teams with a large proportion of unnecessary documents. To the extent certain custodians or groups of documents are more likely to contain relevant content, their review should be prioritised.

In recent years, great advances have been made in the use of predictive coding in e-discovery to more quickly identify relevant documents and reduce the number of non-responsive documents that need to be individually reviewed. In our experience, the judicious use of predictive coding technologies is increasingly acceptable to regulators and prosecutors in the right context, so long as the specific methodologies and rationale for using those tools are clearly discussed with the authorities at the outset. Even in cases where a full human review of a document

15 The HIPAA Rules generally require that covered entities enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. See 45 C.F.R. Part 160 and Part 164.

population is contemplated or required, predictive coding can be a useful tool for internal investigators in locating the most relevant documents quickly, before the full review is complete.

Taking these considerations into account, the investigating attorneys should draft a document review protocol that sets forth in as much detail as possible the purpose of the review, the responsive issues, and how documents should be tagged or marked. Devising the system of tags and codes is a critical step. Counsel should give careful consideration to how they may want to sort the data as the investigation progresses and devise codes that will make that work efficient. On the other hand, counsel should take care not to include so many codes that the review will be unduly slowed or overly confusing to reviewers.

If the need to produce documents to outside parties is likely, responsive documents should be reviewed to see if they are privileged and, if so, which privilege would apply. Disclosure of privileged material to a third party, even the government, can in some instances constitute a waiver of privilege, although steps can be taken to limit the scope of such a waiver.

See Chapter 36 on privilege

In the context of an investigation, gathering material is a dynamic process. Discovery of documents will often require follow-up interviews, and information gleaned in interviews may reveal the need for additional search terms or custodians. Documents retrieved from one custodian may reveal that a previously unknown custodian may have responsive material. The document preservation notice and review protocol should be updated as needed throughout the course of the investigation as this information comes to light.

Documents located abroad 6.7

When documents are located in jurisdictions outside the United States, the first step is to the look at the relevant country's data privacy and bank secrecy laws (or whether blocking statutes or state secrecy laws are implicated), many of which may seem counter-intuitive to US practitioners.[16] In the European Union, for instance, employees' personal data can only be collected and processed under certain conditions, and law firms and their clients must protect this data from misuse and respect certain rights of the individual data owners.[17] These requirements and the penalties for non-compliance have been heightened by the recent implementation of the General Data Protection Regulation (GDPR), which superseded the pre-existing Data Protection Directive governing data privacy and applies directly throughout the European Economic Area. Some countries also have procedural requirements

See Chapter 40 on data protection

16 In some cases, data privacy regimes can also apply to documents located within the United States if the data resides there in connection with the activities of a non-US entity. This is true, for example, of the European Union General Data Protection Regulation, which has extraterritorial effect in certain circumstances.

17 See the EU General Data Protection Regulation adopted in April 2016, which came into effect on 25 May 2018 and superseded the EU Data Protection Directive (Directive 95/46/EC). Other notable data privacy laws include Hong Kong: Personal Data (Privacy) Ordinance (Cap 486); Japan: the Act on the Protection of Personal Information (Law No. 57 of 2003); and Russia: the Russian Federal Law 'On Personal Data' (No. 152-FZ).

(e.g., notification to a works council) that govern the processing, transfer, storage, maintenance and access to documents.[18] Given the heightened scrutiny surrounding personal information, counsel should take care to collect and store only what the investigation requires, and consider whether any special arrangements, such as a cross-border data transfer agreement, would help mitigate collateral risk.

In the past, corporate counsel has sometimes relied on these foreign laws to avoid producing documents located abroad to US authorities. Recently, DOJ officials have expressed increasing scepticism toward explanations that documents cannot be provided to the DOJ in the United States because of data privacy restrictions, and, by virtue of handling many cases implicating foreign laws, have themselves become knowledgeable about their limitations and exceptions. In the DOJ's view, '[c]orporations are often too quick to claim that they cannot retrieve overseas documents, emails or other evidence regarding individuals due to foreign data privacy laws . . . . A company that tries to hide culpable individuals or otherwise available evidence behind inaccurately expansive interpretations of foreign data protection laws places its cooperation credit at great risk.'[19] In 2015, the then head of the Criminal Division at the DOJ, Leslie Caldwell, stated that while 'some foreign data privacy laws may limit or prohibit the disclosure of certain types of data or information,' the DOJ nonetheless will challenge what it perceives to be 'unfounded reliance on these laws' and encouraged companies to refrain from 'making broad "knee jerk" claims that large categories of information are protected from disclosure.'[20] The following year, Caldwell reiterated that the DOJ was leveraging its relationships with foreign enforcement partners 'to obtain information when non-cooperative companies make invalid assertions about particular data privacy laws in an effort to shield themselves from [DOJ] investigations.'[21]

This is not to say that companies should disregard or be cavalier with foreign data privacy laws. But counsel should look for solutions to this issue. Where potential strategies exist – even creative ones – for obtaining relevant documents that are located abroad, United States authorities have clearly indicated they expect companies to do so to receive co-operation credit. This will almost always require coordination with skilled counsel in the relevant jurisdiction where the documents are located.

---

18 See, e.g., articles 91, 96 and 96a of the Austrian Labour Constitution Act (Arbeitsverfassungsgesetz – ArbVG).

19 Remarks by Principal Deputy Assistant Attorney General for the Criminal Division Marshall L. Miller at the Global Investigations Review conference, New York, N.Y., United States, 17 September 2014, available at https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller.

20 Remarks by Assistant Attorney General Leslie R. Caldwell at the Compliance Week Conference (19 May 2015), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-compliance-week-conference.

21 Remarks by Assistant Attorney General Leslie R. Caldwell at the American Bar Association's 30th Annual National Institute on White Collar Crime (4 March 2016), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-american-bar-association-s-30th.

Appendix 1

About the Authors

Bruce E Yannett
Debevoise & Plimpton LLP

Bruce Yannett is deputy presiding partner of the firm and chair of the white-collar and regulatory defence practice at Debevoise & Plimpton. He focuses on white-collar criminal defence, regulatory enforcement and internal investigations. He represents a broad range of companies, financial institutions and their executives in matters involving securities fraud, accounting fraud, foreign bribery, cybersecurity, insider trading and money laundering. He has extensive experience representing corporations and individuals outside the United States in responding to inquiries and investigations.

Chambers Global 2018 recognises Mr Yannett as a Band 1 practitioner for FCPA matters, and *Chambers USA* 2018 recognises Mr Yannett as a Band 1 practitioner for both white-collar criminal defence and FCPA matters. Clients praise his work as 'excellent' and describe him as a 'very strong communicator and litigator' and a 'leading light in the field', noting that 'he has real gravitas about him', giving him the 'immediate respect of everybody in the room'. In a similar vein, *The Legal 500: United States* calls him a 'superstar', *Lawdragon* recognises him as one of the 500 leading lawyers in America, and *Benchmark Litigation* names him a 'Litigation Star'. Further, in selecting Debevoise as 'Litigation Department of the Year' in 2014, *The American Lawyer* stated that Mr Yannett's work on the groundbreaking Siemens FCPA internal investigation, which spanned 34 countries, and settlement with US and German authorities, 'cemented his credibility with regulators' on subsequent matters.

He is a member of the American Law Institute. Mr Yannett is on the board of advisers for the New York University programme on corporate compliance and enforcement.

Early in his career, Mr Yannett served in the Office of Independent Counsel: Iran/Contra and as an assistant United States attorney.

David Sarratt
Debevoise & Plimpton LLP

David Sarratt is a partner in Debevoise's litigation department. He is a seasoned trial lawyer whose practice focuses on white-collar criminal defence, internal investigations and complex civil litigation. Mr Sarratt has significant experience in the technology sector and is recommended by *The Legal 500 US* for cyber law and international litigation (2017).

Prior to joining the firm, Mr Sarratt served as an assistant United States attorney in the Eastern District of New York. As a federal prosecutor, Mr Sarratt supervised and participated in a wide variety of investigations and prosecutions, involving international terrorism, cybercrime, financial and healthcare fraud, racketeering and other crimes. He successfully tried numerous cases to verdict and briefed and argued appeals in the US Court of Appeals for the Second Circuit.

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
beyannett@debevoise.com
dsarratt@debevoise.com
www.debevoise.com