Beware! Whistleblowers, Wolves, and Lambs – Navigating Ethical Landmines in Global Investigations

Paula Howell Anderson, Partner
Shearman & Sterling
New York, NY

Philip Urofsky, Partner
Shearman & Sterling
Washington, DC

PAULA HOWELL ANDERSON is a partner in Shearman and Sterling's Litigation practice. Her experience is broad, with an international focus, and encompasses Foreign Corrupt Practices Act (FCPA) investigations, global anti-corruption, sanctions and AML compliance, complex commercial litigation, cross-border disputes, and M&A-related litigation. She has led monitorship teams for the FCPA compliance monitorships of York International and Baker Hughes, and has conducted anti-corruption investigations in Africa, Asia, Europe, Latin America and the Middle East. Before joining the firm, Ms. Anderson served as a judicial clerk to the Honorable Diane Lebedeff, New York Supreme Court in 1999. In 2012, she was awarded the National Organization of Women's "2012 Women of Power and Influence Award," and was named to Crain's NY Business Magazine's "40 Under 40" list of top achievers under the age of 40. In 2014, Ms. Anderson was named to Global Investigations Review's inaugural "40 Under 40" list of the world's leading investigations specialists. Ms. Anderson has also been recognized by the Council of Urban Professionals ("CUP") as a 2014 CUP Catalyst Change Agent in Law for her extraordinary professional achievements and service to the community. In 2018, she was named one of the Most Influential Black Lawyers by Savoy Magazine.

PHILIP UROFSKY is head of the global anti-corruption practice at Shearman & Sterling LLP, where he counsels Boards, companies, and individuals concerning government investigations, internal investigations, and compliance controls with respect to the Foreign Corrupt Practices Act, financial sanctions regulations, and other white collar laws and regulations. Formerly the lead FCPA trial attorney at the Department of Justice, he was responsible for many FCPA investigations and prosecutions, helped negotiate the Council of Europe and OECD Conventions and was designated as the U.S. expert for the OECD Working Group on Bribery's peer review process, and was the principal drafter of the DOJ's Federal Principles of Corporate Prosecution (the "Holder Memo") (although he disclaims any responsibility for what the government did with it afterwards). Mr. Urofsky writes and speaks widely on topics related to the design and implementation of compliance programs and sanctions and anti-corruption enforcement trends and patterns.

Navigating Ethical Landmines in Global Investigations

You are the compliance officer of a multinational company and, without warning (as usually happens), a whistleblower contacts you and claims that a significant division, with assets and operations overseas and domestic senior management, is rife with corruption and self-dealing. Her allegations are not obviously incredible and have some suggestive details, and you know that they must be investigated. This is not, however, your first rodeo, and you know that the cross-border aspects of this investigation will require careful planning to avoid the pitfalls presented by different legal and labor systems. What are they?

I. Dealing with Whistleblowers

Dealing with whistleblowers can often be frustrating and carries with it significant risks and pitfalls. Whistleblowers often present themselves as "white knights" acting altruistically to protect the company and report wrongdoing. In some cases, that may well be true – and that carries its own risk. "True believers" are loathe to accept any contrary finding of the investigation and may well cry "whitewash" and "cover-up" if your investigation does anything other than corroborate their beliefs. Any indication that you triaged their allegations or prioritized certain allegations while not devoting substantial time to vague or minor allegations may be viewed as a lack of serious commitment to compliance. If you cannot convince the whistleblower that you have followed every lead, weighed all evidence objectively, and assigned culpability without concern for rank or influence, you face a serious risk that the whistleblower may go to the authorities – and that the authorities will find her allegations as facially credible as you did initially. This places you in the awkward position, discussed more *infra* §III, of weighing the pros and cons of making a preemptive voluntary disclosure to the regulators in an effort to influence the narrative.

On the other hand, some whistleblowers come with baggage and agendas. They may be retaliating against supervisors for poor reviews or lack of promotion, they may feel slighted by co-workers, or they may be out for a payday – or some combination of all of the above. While this may all be true, it does not automatically mean that the whistleblowers are lying or making up their allegations. The possibility that a whistleblower may have an agenda is something you must consider in evaluating their allegations, and, if the whistleblower goes to the authorities, it is something you will want to bring to the authorities' attention. However, it is a truism well understood by prosecutors – and therefore also necessarily by you – that merely because a witness has an agenda does not mean they are not telling the truth.

A. Whistleblower Incentives

Virtually any corporate compliance program will encourage employees, and even third parties, to come forward with allegations of wrongdoing. The programs usually offer anonymity or confidentiality and, as discussed below, protection from retaliation. In some instances, they even offer some form of awards or incentives.[1]

Of more concern to you, however, are the incentives offered by the government. In the U.S., the two most prominent are those established under the Dodd-Frank Act[2] covering securities

[1] For example, former investment bank and securities brokerage, Bear Stearns, had implemented a policy to encourage employees to raise concerns, stating, "We want people at Bear Stearns to cry wolf, [and] if the doubt is justified, the reporter will be handsomely rewarded." Examples highlighted to employees included administrative assistants who reported submissions of false expense reports. George E. Murphy, "Using Incentives in Your Compliance and Ethics Program," Society of Corporate Compliance and Ethics (2011), https://assets.hcca-info.org (Search "IncentivesCEProgram-Murphy").

[2] 12 U.S.C. § 53.

fraud and other violations of the securities laws (including the Foreign Corrupt Practices Act (FCPA)[3]) and the *qui tam* statute[4] relating to false claims.

1. Dodd-Frank Act

The Dodd-Frank Act, enacted in 2010, provides that the whistleblower must come forward with "original information."[5] That is, the information cannot be from a government hearing or report, an audit or investigation, or from the news media (unless the whistleblower is the source of the news media). Additionally, were a compliance officer to come forward, the information shared with authorities would need to come from outside of a compliance role to be considered "original information." Further, under Dodd-Frank, a whistleblower is disqualified if convicted of a crime related to the allegation, or if the information provided is not complete.[6]

If the whistleblower qualifies, however, the Dodd-Frank Act requires the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission to reward whistleblowers who come forward with information with 10% to 30 % of the monetary recovery

[3] 15 U.S.C. §§ 78m(b), 78dd-1, and 78ff. The FCPA is part of the Securities Exchange Act of 1934 ("Exchange Act") and prohibits bribery of foreign public officials by companies who qualify as issuers under the Exchange Act and also requires such issuers to maintain accurate books and records and to implement effective internal financial controls. Other provisions of the Act apply to non-issuers and, although codified as 15 U.S.C. §§ 78dd-2 and 78dd-3, are not part of the Exchange Act and are not, therefore, subject to the Dodd-Frank or Sarbanes-Oxley Acts.

[4] 31 U.S.C. §§ 3729 – 3733.

[5] 17 CFR § 240.21F-4(b)(1).

[6] 17 CFR § 240/21F-8.

that the SEC obtains from the offending party so long as the total recovery is over $1 million.[7] As of June 2020, the SEC has awarded approximately $501 million to 85 whistleblowers.[8]

Significantly, from a compliance perspective, a whistleblower is only qualified to be paid a bounty if he or she actually files a report with the SEC. Such a report may be anonymous or made through counsel. This obviously poses a problem for you and your fellow compliance officers, as it appears to discourage internal reporting in favor of going directly to the authorities. The SEC, however, recognized these potential negative incentives and provided that the whistleblower may initially report internally, while maintaining her eligibility for the bounty so long as she reports the information to the SEC within 120 days of reporting it internally.[9] Note that although you may have your suspicions, you may never know if any of your employees made a whistleblower report to the SEC, as the Dodd-Frank Act mandates that the SEC maintain the confidentiality of whistleblowers who disclose information and are in turn rewarded for their disclosures.

2. *Qui Tam* Statute

The *qui tam* statute operates differently. Under that statute, the whistleblower, known as the "relator," first files a sealed civil complaint in the name of the United States alleging that the defendant committed some form of fraud upon the U.S. government by making false claims.[10] "False claims" in this context is a term broadly construed and encompasses the following:

---

[7] 15 U.S.C. § 78u-6.

[8] Press Release, SEC, SEC Awards $125,000 to Whistleblower (June 23, 2020), https://www.sec.gov (search "Press Release").

[9] *See* 17 CFR §240.21F-4(b)(7) and 17 CFR §240.21F-4(c).

[10] 31 U.S.C. §§ 3729 – 3733.

> (1) [P]resenting a false claim; (2) making or using a false record or statement material to a false claim; (3) possessing property or money of the U.S. and delivering less than all of it; (4) delivering a certified receipt with intent to defraud the U.S.; (5) buying public property from a federal officer or employee who may not lawfully sell it; (6) using a false record or statement material to an obligation to pay or transmit money or property to the U.S., or concealing or improperly avoiding or decreasing an obligation to pay or transmit money or property to the U.S.; (7) conspiring to commit any such offense.[11]

The relator then must provide a copy to the Department of Justice (DOJ) which then has the right to take over the civil case.[12] If, however, it declines to do so, the relator may pursue the litigation at his or her own expense. In both cases, the relator will be entitled 15% to 25% of any award the government receives if the defendant is found to have filed false claims with the government – with, of course, a greater payout in the latter case if he had to litigate at his own expense.[13] A significant difference between the *qui tam* bounty and that under Dodd-Frank is that whistleblowers under the *qui tam* statute recover their share irrespective of how much the government recovers. Further, in contrast to the *qui tam*, the Dodd-Frank bounty generally excludes those serving in a compliance function.[14] According to the DOJ, there were 633 *qui tam* suits in the 2019 fiscal year, and the DOJ estimates that it has recovered over $2.1 billion from these and earlier filed suits.[15]

---

[11] Charles Doyle, *Qui Tam: The False Claims Act and Related Federal Statutes*, CONGRESSIONAL RESEARCH SERVICE (2009).

[12] The *qui tam* suits are civil matters. However, a parallel criminal investigation may put pressure on a company to self-report such civil liabilities.

[13] 31 U.S.C. §3730(d).

[14] *See* § I.A.1.

[15] Press Release, U.S. Dep't Justice, Justice Department Recovers Over $3 Billion from False Claims Act Cases in Fiscal Year 2019 (Jan. 9, 2020), https://www.justice.gov (search "PR").

B. Protection against Retaliation

As a compliance officer, you must also be sensitive to the risk that any action your employer takes with respect to the whistleblower could be perceived as retaliation. Again, most corporate compliance programs assure whistleblowers that the company will not tolerate retaliation and that the company itself will not take any adverse employment action even if the whistleblower's allegations prove to be unfounded, provided that they were made in good faith.[16] Companies that violate their own policies in this respect may subject themselves to potential liability under various legal theories. However, particularly with respect to issuers, federal law has imposed additional legal risks.

1. Sarbanes-Oxley Act

The Sarbanes-Oxley Act, enacted in 2002, is mostly known for its requirement of rigorous internal controls, but it also includes whistleblower provisions.[17] Under the Sarbanes-Oxley Act, employees of public companies who are retaliated against because of disclosures related to mail, wire, bank, or securities fraud have a civil cause of action.[18]

To qualify for protection under Sarbanes-Oxley, the whistleblower must file a written complaint with the Occupational Safety and Health Administration (OSHA), part of the

[16] For example, Sociedad Quimica y Minera de Chile's (SQM) Code of Ethics, available online, includes a Non-Retaliation Policy that states, "Anyone that voices their concerns in good faith will be protected against acts of retaliation….Retaliation against reporting employees is itself a violation of this Code and will be investigated and disciplined when substantiated….A report does not necessarily need to be substantiated for it to be made in good faith, but the reporter should believe it to be a genuine concern of potential misconduct." https://www.sqm.com (search "SQM-Codigo-de-Etica_English").

[17] 18 U.S.C. §1514A.

[18] *Id.*

Department of Labor, within 180 days of the alleged retaliation.[19] If OSHA finds that the complaint has merit, it can order certain remedies which can be challenged by the employer administratively and ultimately in court. If OSHA fails to act in a timely manner (which is often the case) or does not find the complaint to have merit, the employee may then sue in court.

To establish a Sarbanes-Oxley retaliation claim, a whistleblower must show (1) she is an employee engaged in protected whistleblower activity; (2) her employer took adverse employment action against her; and (3) her whistleblower activity, at least partly, caused the adverse employment action.[20] The cumbersome nature of this process meant that it was not particularly useful in complex matters.

Interestingly, despite the fact that many issuers are multinational and operate in an era of globalization, there are territorial limits to the Sarbanes-Oxley protections. Thus, a recent decision by the Department of Labor's Administrative Review Board (LARB) found that Sarbanes-Oxley's anti-retaliation provisions do not apply extraterritorially. In the decision, the LARB dismissed the

[19] OSHA, OSHA Fact Sheet: Filing Whistleblower Complaints under the Sarbanes-Oxley Act, https://www.osha.gov (search "Osha Fact Sheet"). OSHA covers all U.S. workers not otherwise preempted by another federal statute. While there are federal statutes relevant to certain extraction industries, such as the Federal Mine Safety and Health Act (governed by the Mine Safety and Health Administration (MSHA)), the line between OSHA and MSHA is not always clear, in part because most mining companies likely have activity covered by both OSHA and MSHA. Brad Hiles and Ben McMillen, *Interagency Agreement: MSHA and OSHA*, ROCK PRODUCTS (Nov. 16, 2016), http://www.rockproducts.com (search "The Blurred Line"). The division between OSHA and MSHA is beyond the scope of this article, as is analysis of any other federal and state laws containing protections against retaliation that may apply to the mining industry.

[20] *Id.*

anti-retaliation case brought by the "Hong Kong-based employee of a foreign subsidiary of the Respondent, who worked entirely outside of the United States."[21]

2. Dodd-Frank Act

The Sarbanes-Oxley mechanism was ultimately viewed as overly cumbersome and did not provide incentives to report. The Dodd-Frank Act sought to correct these shortcomings by creating a self-executing whistleblower protection that provided whistleblowers with a private cause of action in the event that they were discharged or discriminated against by their employers.[22] Termination is not necessary (or sufficient) for a successful retaliation claim.[23] However, under Dodd-Frank, a whistleblower does not have legal protection until she reports to the SEC, as opposed to merely reporting internally to the company.[24] Further, any action taken by a company before a whistleblower reports would not be considered retaliation, even if the whistleblower eventually reports to the SEC.[25] Unlike Sarbanes-Oxley, there have been no cases thus far holding that the Dodd-Frank anti-retaliation provisions do not apply exterritorialy.

The SEC can also bring its own enforcement action for retaliatory behavior under Dodd-Frank. Such enforcement action can result in fines levied upon the company. [26] Furthermore, any

---

[21] Order Dismissing Complaint, Christopher Garvey v. Morgan Stanley, Docket No. 2017-SOX-00030 (Dep't of Labor Feb. 13, 2020).

[22] SEC, "Whistleblower Program," https://www.sec.gov (search "Whistleblower").

[23] 15 U.S.C. § 78u-6.

[24] *See* Dig. Realty Tr. Inc. v. Somers, 137 S. Ct. 2300 (2017).

[25] 15 U.S.C. § 78u-6.

[26] *See*, e.g., Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, In the Matter of International Game Technology, File No. 3-17596 (SEC Sept. 29, 2016).

such retaliation enforcement action by the SEC may also result in the company facing heightened scrutiny from various other government regulators.

C. Examples from Other Jurisdictions

While this article focuses primarily on U.S. law, your response to a whistleblower must also take into account whistleblower regulations in other jurisdictions outside the U.S., particularly if your company has employees (and thus potential whistleblowers) spread across the globe. A brief overview of whistleblower protections and rewards in the U.K., South Africa, and Canada follows.

1. U.K.

The whistleblowing framework in the U.K. is governed by the Public Interest Disclosure Act 1998 (PIDA), which amended the Employment Rights Act 1996 (ERA).[27] Former and current employees are protected from adverse employment action, as well as freelancers.[28] However, only disclosures relating to specific categories of information are protected, including: criminal wrongdoings, violations of legal obligations, miscarriages of justice, health and safety hazards, or environmental damage.[29] This is in contrast to the whistleblowing framework in the U.S. which generally does not have subject matter limitations.

2. South Africa

The whistleblowing framework in South Africa includes constitutional provisions, the Protected Disclosures Act 2000 (PDA), the Labor Relations Act (LRA), and the Companies Act

[27] Employment Rights Act 1996, c. 18, (Eng.).

[28] *Id.*

[29] Employment Rights Act 1996, c. 18, § 43B (1), (Eng.).

2008 (CA).[30] The PDA protects whistleblowers from any form of adverse employment action.[31] While protection under the PDA and LRA is limited to employees, the CA extends whistleblower protection to contractors as well.[32] However, like the U.K., only disclosures relating to specific categories of information are protected, including: criminal wrongdoings, violations of legal obligations, miscarriages of justice, health and safety hazards, unfair discrimination, or environmental damage.[33]

3. Canada

In Canada, whistleblower protection is primarily provided under the Criminal Code. Under Section 425.1 of the Criminal Code, employers may not threaten to, or take, disciplinary action, demote, or terminate with the intent to force the whistleblower to refrain from providing information to law enforcement officials.[34] Further, employers may not retaliate against a whistleblower who has already provided such information.[35] However, Section 425.1 applies only to whistleblowers who report to law enforcement officials rather than just reporting internally to the company.[36] Aside from the Criminal Code, there are also whistleblower provisions in other

[30] Protected Disclosures Act 26 of 2000 (S. Afr.); the Labor Relations Act 66 of 1995 (S. Afr.); Companies Act 71 of 2008 (S. Afr.).

[31] Protected Disclosures Act 26 of 2000 (S. Afr.).

[32] Companies Act 71 of 2008 (S. Afr.).

[33] Protected Disclosures Act 26 of 2000 (S. Afr.).

[34] Criminal Code, RSC 1985, c C-46, s 425.1.

[35] *Id.*

[36] *Id.*

statutes, primarily at the provincial level. These protections typically relate to specific areas, such as occupational health and safety hazards or environmental protections.[37]

D. Related Risks

The importance of protecting whistleblowers from retaliation cannot be disputed. The risk, however, is that these protections can be more than a shield and can become a sword in the hands of the whistleblower who can claim that any action he or she perceives as negative – such as a deservedly negative performance review, perceived cold shoulders from co-workers, or even routine but undesirable assignments or reassignments – is retaliatory. This risk is both real and potentially costly, as a number of recent examples demonstrate.

1. SandRidge Energy Inc.

In 2016, the SEC settled charges with SandRidge Energy Inc., an oil-and-gas company, alleging that SandRidge used illegal separation agreements and retaliated against a whistleblower.[38] The SEC found that SandRidge, after a new whistleblower protection policy went into effect, continued to ban departing employees from participating in government investigations or from disclosing information about the company.[39] Further, the SEC found that SandRidge fired a whistleblower who raised concerns about how oil-and-gas reserves were being calculated and publicly reported and, although it began in internal audit, did not complete it and

[37] *See, e.g.*, Ontario's Occupational Health and Safety Act, R.S.O. 1990, c. O.1 (Can.) and Human Rights Code, R.S.O. 1990, c. H. 19 (Can.).

[38] Press Release, SEC, Company Settles Charges in Whistleblower Retaliation Case (Dec. 20, 2016), https://www.sec.gov (search "SandRidge").

[39] *Id.*

did not conduct an investigation of the whistleblower's allegations.[40] Without admitting or denying the SEC's findings, SandRidge agreed to pay a $1.4 million penalty, pending the company's bankruptcy plan.[41]

2. Walmart

In 2019, Walmart entered into a global settlement with the DOJ and SEC for $282.7 million for failing to implement and enforce an adequate anti-corruption compliance program under the FCPA.[42] In late 2011, Walmart learned that the New York Times was investigating Walmart's decision to shut down that investigation[43] and, shortly thereafter, informed the DOJ that it had initiated an internal investigation into possible FCPA violations related to obtaining permits and disclosed the internal investigation in SEC filings.[44] In April 2012, the New York Times published an expose with allegations of widespread corruption and bribery at Walmart.[45] After an investigation spanning seven years and multiple jurisdictions, Walmart entered into a settlement with the DOJ and SEC. One member of Walmart's ethics and compliance division, Shane Perry, claims that he was tasked with investigating potential violations in Mexico in June 2011, and

---

[40] *Id.*

[41] *Id.*

[42] Press Release, SEC, Walmart Charged With FCPA Violations (June 20, 2019), https://www.sec.gov (search "Walmart Charged With FCPA Violations"); Press Release, Walmart, Walmart Reaches Agreements with the DOG and the SEC to Resolve Their FCPA Investigations (June 20, 2019), https://corporate.walmart.com (search "Walmart Reaches Agreements").

[43] David Barstow, *Wal-Mart Hushed Up a Vast Mexican Bribery Case*, N.Y. TIMES (Apr. 21, 2012), https://www.nytimes.com (search "Walmart Hushed Up Mexican Bribery").

[44] *Id.*

[45] *Id.*

despite submitting his investigation report in November 2011, management did not comment on his findings for five years.[46] Perry alleges that he was questioned about his report in February 2017, and subsequently fired for refusing to make changes to it.[47] Walmart has denied these allegations.

3. Rio Tinto

Rio Tinto, among the world's largest mining companies, found itself in hot water after a series of leaked emails detailed top executives discussing a payment of $10.5 million made to François Polge de Combret, a consultant who helped secure rights to an iron-ore deposit in Guinea.[48] The emails, which sparked an internal investigation, were from 2011 and were leaked in August 2016 when they were posted anonymously on the internet. The internal investigation raised questions about whether the company's internal compliance procedures were being followed. By November 2016, Rio Tinto announced it had suspended its Head of Energy and Minerals, as well as its Head of Legal and Regulatory affairs.[49] Rio Tinto then voluntarily disclosed information about the payment to authorities in the U.S., U.K., and Australia.[50]

---

[46] Complaint, Perry, et al., v. Walmart Stores, Inc., et al., No. 04CV-20-1150 (Ark. Cir. Ct. May 7, 2020).

[47] *Id.*

[48] Camilla Hodgson, *'This is not a standard situation:' Read the emails between Rio Tinto executives that sparked a corruption investigation*, BUSINESS INSIDER (July 25, 2017), https://www.businessinsider.com/rio-tinto-guinea-leaked-executive-emails-corruption-investigation-2017-7.

[49] Perry Williams, et al., *Rio Tinto Fires Two Senior Executives Amid Payment Probe*, BLOOMBERG, (NOV. 16, 2016), https://www.bloomberg.com/news/articles/2016-11-16/rio-tinto-fires-energy-chief-alan-davies-after-simandou-probe.

[50] "*Rio Tinto Annual Report*" (2017), https://www.sec.gov/Archives/edgar/data/863064/000156459018004161/ex15.htm.

II. Investigating the Whistleblower Report and Conducting an Internal Investigation

Once you have determined that the whistleblower allegations are facially credible, you will need to initiate your company's procedures for conducting an internal investigation. Not only is an investigation good practice for ensuring that the company is in compliance with the law, but enforcement agencies often cite internal investigations as part of a company's cooperation with a government investigation. In some jurisdictions, an investigation may be required by law. For instance, in Delaware and other jurisdictions in the U.S., a company's directors and officers have a duty of loyalty, a duty of care, and a duty of disclosure. Under the duty of loyalty, directors and officers are expected to act without any conflict of interest derived from a material personal financial interest in the matter at issue.[51] Under the duty of care, directors and officers are expected to be informed and act in a deliberative manner. Under the duty of disclosure (or "duty of candor"), directors and officers are expected to disclose material information within their control to shareholders. Any one of these duties potentially implicates the responsibility of the company's directors to ensure that the company has adequate procedures and internal controls to both prevent and detect misconduct. Failure to fulfill these duties may result in civil liability for breach of fiduciary duty or corporate waste, or in some cases, criminal charges for fraud.[52]

Internal responsibility for managing the investigation must be assigned at the outset of the investigation. Whether senior management, the Board, or one of the Board's committees, such as the Audit Committee or, in appropriate circumstances, a specially mandated independent committee, manages the investigation will depend on the nature and seriousness of the alleged

[51] *See* In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

[52] Paula Anderson & Claudius Sokenu, *How a skilled board should manage an internal investigation*, DIRECTORS & BOARDS (First Quarter 2015), at 36, 37.

wrongdoing, who is involved in the alleged conduct, and the degree of independence necessary to conduct an impartial investigation. For instance, if a senior executive appears to be involved in the alleged misconduct, independent directors may need to oversee the investigation to prevent the appearance of a conflict of interest and the executive will need to be excluded from any discussions about the investigation. At the operational level, multiple teams play a role in internal investigations, including Compliance, Internal Audit, Human Resources, Legal, Business, and IT. To ensure that these teams coordinate their efforts, the company should ensure that a point person has both the responsibility and the authority to ensure the investigation runs smoothly.

One very important consideration for a company at the outset of an internal investigation is determining whether external counsel should be retained. It is important to consider how the investigation may eventually be perceived by enforcement agencies and the media. There are obvious advantages to using counsel who is familiar with the company and its operations, and the fact that counsel or other members of her firm may have done other work for the company does not automatically mean that her investigation would be viewed as biased or compromised. Another consideration is the cost of external counsel compared to in-house counsel and other internal resources. Nevertheless, the company must weigh the efficiency and cost considerations against the value of perceived objectivity and independence and, sometimes, the genuine need for special legal expertise. For example, a company must consider if there is a potential conflict of interest faced by in-house or external counsel. In the Walmart case discussed in Section I.D., the whistleblower identified the General Counsel in Mexico as being part of the alleged conspiracy. However, according to the New York Times, the company nevertheless assigned responsibility for investigating the allegations to that same General Counsel, with obvious consequences in the subsequent government investigation.

A. Document Retention

Once a company becomes aware of an allegation that is sufficiently credible such that it is reasonably foreseeable that the government may eventually become involved, it should take concrete, documented, and verifiable steps to ensure preservation of evidence and avoid claims of inadvertent or, worse, deliberate spoliation. This is not only good practice but also a legal obligation once the company becomes aware of a government investigation.[53] John Haried, the Criminal eDiscovery Coordinator and the Co-chair of the eDiscovery Working Group for the Executive Office of U.S. Attorneys in the DOJ, has stated that the DOJ is "very serious about prosecuting cases where there is destruction of evidence, because it's been a problem in the past."[54] The U.K.'s Serious Fraud Office (SFO) released Corporate Cooperation Guidance in August 2019 that outlined its expectations for companies' retaining and providing documents to the SFO. The guidance instructs companies to preserve digital and hard copies of relevant documents "using a method that prevents the risk of document destruction or damage."[55] Companies must inform the SFO if it suspects that documents have been lost, deleted, or destroyed for any reason.[56]

As an initial step, it is important to understand what document preservation policies are in place, and if a company has retained outside counsel, it is important that outside counsel

---

[53] 18 U.S.C. § 1519 (making it a crime if anyone "knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation…").

[54] Gavin Broady, *DOJ Chiefs Share The Wrong Way To Respond To A Subpoena*, LAW360, Feb. 5, 2015, https://www.law360.com (search "DOJ Chiefs Share Wrong Way To Respond To Subpoena").

[55] SFO Operational Handbook, *Corporate Co-operation Guidance*, SFO (Aug. 16, 2019) at 2, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/#.

[56] *Id.*

understand the policy as well. Next, it is critical to learn the system architecture, data storage, and device management. This includes how a company stores emails (including deleted emails) and instant messages.

The next necessary step to properly preserve documents is the issuance of a litigation hold notice. The notice should cover the retention of personal and work emails, documents saved on share folders, databases, hard drives, and computers, and messages and information stored on hand-held devices, both personal and company-issued. It is generally best practice that the notice should cover personal and work emails, shared folders, databases, hard drives, computers, and hand-held devices.

One issue that has received increased attention in recent years is whether companies are required to retain "ephemeral" text messages and instant messages, such as those sent through the popular applications Slack, WhatsApp, and WeChat, even before an investigation is initiated. In 2017, the DOJ sought to label such messages as business records and attempted to make retention of such messages a condition of cooperation for an investigation, even if the messages were sent before the investigation began.[57] The DOJ subsequently backed away from the policy after a hail of criticism.[58] In light of the revisions to the DOJ's policy, a company now faces a cost-benefit balance when considering retaining large amounts of data for which it has no business need.

[57] USAM § 9-47.120 (2018).

[58] *FCPA Digest: Recent Trends and Patters in the Enforcement of the Foreign Corrupt Practices Act*, SHEARMAN & STERLING LLP (2019); Derek Hahn, et al., *Clarifications Needed After DOJ's New FCPA Policy*, LAW360, Mar. 22, 2019, https://www.law360.com (search "New FCPA Policy Clarifications") (Critics claimed the policy was vague and could have been read to prohibit the use of ephemeral messaging, whether or not the messaging related to company information.).

Perhaps this need to balance explains the increasing popularity of messaging platforms like Slack, which offer different retention-length customization for private direct messages versus public channel messages.[59] However, in cases where bad faith may be suspected around missing text messages and other electronic information, such as the intentional wiping of cellphones and laptops, spoliation sanctions may be imposed.[60]

The breadth of the hold notice will depend on the alleged misconduct. Whether the request extends beyond current employees will depend on when the alleged misconduct took place and whether former employees were involved in the alleged misconduct. It is critical to understand – and help your employees understand – that retention has nothing to do with culpability; it is simply a means of preserving relevant evidence. That said, it is certainly important to preserve the data of potentially culpable employees which may mean that you preserve the data not only of the apparently responsible employees but also of employees two levels above and below those employees both to detect additional culpable employees and to capture emails or other data that culpable employees might have tried to delete. Additionally, employees should be required to provide an acknowledgment of the notice.

B. Document Collection and Review

In the U.S., there are very few limits on a company's ability to collect and review its employees' data.[61] This extends not only to data on company-owned devices, but also, as a

[59] *Customise message and file retention*, SLACK (2020), https://slack.com (search "Customise message").

[60] Southeastern Mech. Servs. v. Brody, 657 F. Supp 2d 1293 (M.D. Fla. 2009) (held that the intentional wiping of personal Blackberries of all text messages, emails, and applications by defendants was spoliation and subject to sanctions).

[61] Casey C. Sullivan, *When Can You* Obtain *Discovery Into Employees' Personal Devices?* LOGIKCULL (Feb. 22, 2018), https://www.logikcull.com/blog/when-can-you-obtain-discovery-into-employees-personal-devices

practical and legal matter, to private devices, given that business is increasingly being conducted on personal devices.[62] Further, cooperation with a company's internal investigation, at the risk of termination, is a given under most U.S. employment contracts and substantive employment law.[63]

In Europe and increasingly in other countries, the story may be quite different. Collection and review of an employee's emails may run full tilt into the EU's General Data Protection Regulation (GDPR) as well as local labor laws and practices, including, in some countries, works councils, as well as, to a lesser extent, blocking statutes. In addition, surprisingly to some American practitioners (and many prosecutors), foreign corporate governance principles may limit the ability of the parent corporation to direct the investigation at the subsidiary level. In this section, we will discuss these issues and potential strategies you may consider to overcome them.

1. Data Protection

In effect since May 25, 2018, the GDPR replaced the earlier EU Data Protection Directive and sets regulations for organizations that process personal data of EU citizens or residents.[64] Although not geared directly towards internal investigations by an employer, aspects of the GDPR's protections have obvious implications for data collection, processing, review, and disclosure in that context. Major protections offered to EU citizens and residents include transparency on whether data processing is occurring and for what legitimate purpose. Incorporated within transparency is the mandate to gather and document "freely given, specific,

---

[62] *Id.* Though many companies do urge employees to use only company phones and email for business use to avoid this problem.

[63] Testimony of Henry W Asbill, National Association of Criminal Defense Lawyers, to the US Sentencing Commission, at 4 (Nov. 15 2005) https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/special-reports/11-15-05/Asbill.pdf.

[64] *What is GDPR, the EU's new data protection law?*, GDPR, https://gdpr.eu (search "What is GDPR").

informed, and unambiguous" consent by data subjects prior to processing that data subject's data except in limited circumstances.[65] Consent requests must be presented without distractions or obstructions in "clear and plain language," and data subjects can withdraw consent at any time and demand their information be deleted (*i.e.*, the "right to be forgotten").[66] Organizations must also minimize the amount of data collected, maintain collected data's accuracy, and limit data storage to only "as long as necessary for the specified purpose."[67] Additionally, data security, integrity, and confidentiality must be ensured by processing organizations and can be done via methods such as end-to-end encryption and two-step verification. Organizations are responsible for establishing and maintaining the ability to demonstrate GDPR compliance with all the above mandates.

Although official EU guidance on preserving privacy during document collection and review in the course of, or even in anticipation of, an investigation is limited, the Information Commissioner's Office (ICO), an independent public U.K. body that reports directly to parliament on how to uphold information rights, has provided some advice for how organizations should set up or update their document retention periods in accordance to the GDPR. Some recommendations include reviewing stated purposes for data collection and discerning what information is needed to record a relationship between the organization and employees or fulfill government regulatory requirements.[68] The ICO also recommends comparing information kept for potential legal claims with the current viability of said claims (*e.g.*, 'has the statute of limitations expired for a possible

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Guide to Data Protection*, U.K. Information COMMISSIONER'S OFFICE, https://ico.org.uk (search "Data Protection").

future claim?'), with a strict reminder that future legal claims must be probable and not "just in case" scenarios.[69] When data is being shared between parties, agreements should be drafted that explicitly state what happens if data no longer needs to be shared – *i.e.*, data is returned to the original organization with no copies retained or data is destroyed.[70] Organizations also need to nimbly respond to an individual's invocation of his/her 'right to be forgotten,' by being prepared to determine if there's a clear, legitimate reason to keep their data and how access to retained data will be given to the individual in question.[71]

While the U.S. has fewer restrictions on data collection and review, the GDPR provides a helpful framework. It is a rare case where data considered most sensitive under the GDPR (data related to race, gender, sexual preference, religious beliefs, and political activity) will be relevant to an internal investigation and thus, even in the U.S., basic best practices call for developing narrowly tailored search terms to exclude such data from the review dataset. Indeed, although not legally required, it is generally good practice for companies in the U.S. to narrow the scope of the review to relevant matters if for no other reason but to save costs and ensure that the investigation can be completed in a timely and efficient manner. For instance, investigations involving large numbers of custodians and communications with multiple counterparties that span many years can result in hundreds of thousands of documents to review. It is important to limit custodians to key individuals, create targeted searches, and focus on the alleged misconduct. U.S. companies could use the GDPR as a model for designing their company-wide data protection policies, avoiding the

[69] *Id.*

[70] *Id.*

[71] *Id.*

need to create country-specific policies, which in turn would aid in streamlining internal investigations.[72]

The GDPR places strict limits on disclosing protected information to third parties outside of the EU, including foreign governments absent a government-to-government request and agreement. Thus, as you progress through your investigation, you need to consider what information may ultimately be produced to the foreign enforcement authorities, including the U.S. DOJ and SEC, and in what form, including with what level of redaction. However, the SEC or DOJ, while recognizing the difficulties the GDPR imposes on companies seeking to cooperate, are also skeptical of companies that raise data privacy laws as a blanket excuse to get out of producing documents. Thus, if considering withholding any materials the company should describe any documents impacted by data privacy laws that are not being produced, but should not misrepresent or exaggerate. For example, according to the DOJ, BNP Paribas allegedly violated the International Emergency Economic Powers Act and the Trading with the Enemy Act by moving money through the U.S. banking system on behalf of foreign entities from Sudan, Iran, and Cuba – entities subject to U.S. economic sanctions. According to the Statement of Facts, once U.S. authorities began pursuing BNP Paribas, BNP Paribas did not initially cooperate and purportedly relied on an overly broad section of data privacy laws in Switzerland as precluding BNP Paribas's ability to turn over certain materials, which was weighed against BNP Paribas's other cooperation efforts in the case.[73] Another such case involved Bank Hapoalim, which, in 2020, settled with

[72] Liam Tung, *GDPR, USA? Microsoft says US should match the EU's digital privacy law* (May 21, 2019), https://www.zdnet.com (search "GDPR, USA?").

[73] Statement of Facts, U.S. v. BNP Paribas S.A., Case No. 14-cr-460 (S.D.N.Y. June 30, 2014), Dkt. 13-2, ¶ 72; Press Release, U.S. Dep't Justice, BNP Paribas Sentenced for Conspiring to Violate the International Emergency

U.S. federal authorities for its role in a tax-evasion scheme. As the DOJ explained, "[b]oth the penalty and fine amounts take into consideration that the Bank, after initially providing deficient cooperation through an inadequate internal investigation and the provision of incomplete and inaccurate information and data to the Government, thereafter conducted a thorough internal investigation, provided client-identifying information, and cooperated in ongoing investigations and prosecutions."[74]

2. Data Protection Officers and Works Councils

In some ways, document collection could be considered an extension of document retention and litigation holds. For instance, document collection is a means of ensuring that data is preserved and removed from the custody of those whose actions are the subject of the inquiry. However, some jurisdictions may consider document collection as a more intrusive act that requires notifying, and gaining approval from, data protection officers or works councils. This may be particularly true in certain European countries, notably Germany, where works councils have significant influence on corporate actions as a means of protecting employees' rights. It should not be assumed that either data protection officers or works councils will automatically block document collection requests as European data protection laws note that employees' rights should be weighed against company's legitimate business interests or legal obligations.[75] However, given

Economic Powers Act and the Trading with the Enemy Act (May 1, 2015), https://www.justice.gov (search "BNP Paribas Sentenced for Conspiring").

[74] Press Release, U.S. Dep't Justice, Israel's Largest Bank, Bank Hapoalim, Admits to Conspiring with U.S. Taxpayers to Hide Assets and Income in Offshore Accounts (Apr. 30, 2020), https://www.justice.gov (search "Bank Hapoalim").

[75] Recital 47 of the GDPR.

their role, it is advisable to ensure that any collection is cleared through data protection officers and, where necessary, works councils be consulted before the document collection process begins. Such consultation may need to be performed repeatedly, as the investigation expands or changes focus based on newly discovered evidence or allegations. Of course, this may become even more important as the investigation progresses from collection to processing and review.

3. Blocking Statutes

Another important consideration in document collection is the applicability of blocking statutes. Blocking statutes protect one jurisdiction from the application of another country's extraterritorial laws. Blocking statutes can complicate gaining access to information in a U.S.-based internal investigation and can even impose sanctions if violated.[76] There are a number of examples and counter examples that demonstrate this risk. First, there is the French blocking statute that prohibits producing evidence for U.S. litigation.[77] While this blocking statute is not necessarily relevant to an internal investigation, it poses a difficulty if a company later wants to produce evidence from the investigation to the U.S. government. One possible way around this limitation, similar to data protection, is to gather the material and then assist the U.S. Government in making a request pursuant to a mutual legal assistance treaty.[78] Second, there are laws like the Swiss blocking statute which prohibit conducting investigations on behalf of a foreign power,[79] a risk that has recently become even more pronounced as some U.S. courts have suggested that

[76] *See*, *e.g.*, Council Regulation (EC) No 2271/96 of 22 Nov. 1996.

[77] French Law No. 68-678 of 26 July 1968.

[78] Note, however, there is an example of a U.S. District Judge, Judge Rakoff in the Southern District of New York, refusing to enforce the French blocking statute because the French never enforced it. Motorola Credit Corp. v. Uzan, 73 F. Supp. 3d 397, 403 (S.D.N.Y. 2014), *on reconsideration*, 132 F. Supp. 3d 518 (S.D.N.Y. 2015).

[79] Article 271 of the Swiss Penal Code.

corporate internal investigation are sometimes too closely tied to and even directed by U.S. prosecutors.[80] Relatedly, there is the China National Security Law which requires approval by the government before any company (or individual) within the People's Republic of China can provide evidentiary materials to any foreign power.[81] While this law, and the Swiss blocking statute, may not seem relevant for an internal investigation, the lines can be blurred.

The risks (and protections) of a blocking statute may also be implicated inadvertently if the company and counsel do not pay attention. For example, if a company or its counsel moves data from a foreign jurisdiction to the U.S., the data could be subject to a U.S. subpoena, at which point, a U.S. court could compel discovery even if a blocking statute in the data's originating jurisdiction would not have permitted the discovery.[82] Thus, best practice may be to obtain the data for review within the data's originating jurisdiction.[83]

4. Corporate Governance

Investigators (and compliance officers) conducting an investigation into conduct that spans borders and involves multiple entities within a multinational corporate structure may encounter

[80] U.S. v. Connolly, 2019 WL 2120523 (S.D.N.Y. 2019).

[81] Law of the People's Republic of China on International Criminal Judicial Assistance (promulgated by the Standing Committee of the Thirteenth National People's Congress, Oct. 26, 2018, effective Oct. 26, 2018), ch. I, art. 4, J.A. 355.

[82] *See*, *e.g.*, In re Grand Jury Subpoenas Dated Mar. 19, 2002 & Aug. 2, 2002, 318 F.3d 379 (2d Cir. 2003) (relating to Swiss bank records that a law firm brought into the U.S. Judge Chin concluded that the subpoenaed bank records were not work product because they were "pre-existing records of third parties, created and maintained in the ordinary course of business by those third parties without any reference to litigation whatsoever.").

[83] Philip Urofsky & Grace Harbour, "Internal Investigations & Oversight: Corporate Communications," 2 *Bloomberg Law Review* No. 8 (2009).

other obstacles arising from European corporate governance principles. Unlike in the U.S., parent companies in Europe have limited ability, at least under the strict letter of the law, to direct actions by their subsidiaries, even those related to cooperating with an internal investigation or providing compliance-related information to the parent. Even in cases in which the parent company owns 100% of the subsidiary and appoints the subsidiary's management or supervisory board, the individual board members have a fiduciary duty to the subsidiary and may be held liable for acting against its interests. Granted, in that instance, there does not seem to be a shareholder who would seek to hold them liable for cooperating with the parent's request, but there may be circumstances in which that personal liability may be viewed as a realistic risk, such as where the subsidiary operates in a regulated industry or where the subsidiary is in bankruptcy and pursues claims against the parent or its officers and directors on behalf of the bankruptcy estate. In cases where there are minority shareholders or joint partners, the risk could increase. As such, in conducting an internal investigation, the parent company should anticipate such issues and may, in appropriate circumstances, pose any requests for data preservation, collection, and processing, as well as for interviews in a manner that respects the formalities of corporate governance structures.

5. Document Review

Once preserved and collected, the next step is to identify which datasets need to be processed and reviewed. The first step in a document review process is to formulate search terms to apply to the collected documents. As an initial matter, these searches may be centered around the conduct or the document raised by the whistleblower. However, applying search terms should be a dynamic process such that search terms are updated as more details or information are uncovered. Further, when reviewing documents, *any* problematic documents should be noted, whether the documents relate to the conduct raised by the whistleblower or not.

Separate from email and other document review, in some cases, particularly where the misconduct may involve tax or financial fraud, the company may need to engage a forensic accountant, preferably under the instruction of counsel, to assist in analyzing the company's books and records to identify irregularities. A company or outside counsel should retain a forensic accountant early on in the investigation if a close analysis of the company's books and records is central to the questions at hand in the investigation.[84]

C. Interviews

Interviews pose some of the same issues as document preservation and collection, particularly with respect to labor issues. Again, the contrast between U.S. and foreign practices will be striking, and even stunning, to a U.S. practitioner. In the U.S., the employee is essentially faced with the choice of agreeing to be interviewed, often without counsel present,[85] or being fired for lack of cooperation. In Europe, investigators may face very different circumstances, and employees may have significantly more rights to refuse to be interviewed or to insist on both substantive and procedural protections with respect to the conduct of such interviews. For example, in some countries, even the conduct and subject matter of interviews may require at least notice, if not more, to the works council, which presents obvious risks to both the confidentiality

[84] Rebecca Fitzhugh, *What Is a Forensic Accountant?*, ABA (Jan. 19, 2019), https://www.americanbar.org (search "Forensic Accountant").

[85] We are not suggesting this is necessarily the best or most effective practice but only that it is permitted under the law and reflective of a common practice. Certainly, this practice may be affected by contract, whether by collective bargaining or, for executives, employment contracts. In addition, in many cases, investigative counsel may find it helpful to provide employees with at least "pool counsel" as a means of ensuring employees have a means to obtain advice (and thus not blurring company counsel's role) and ensuring that such employees are prepared to answer questions in an interview in an efficient manner.

and comprehensiveness of the investigation. In France, companies are encouraged to inform employees of their right to retain counsel for their interview if there is a possibility they can be held accountable for wrongdoing, and it is recommended that employees be allowed to review and sign their statements if there is a transcript of the interview.[86] In the U.S., similar practices are discouraged, partly to protect the witness.[87] Further, in many countries, the key leverage over a witness – sit for the interview and be truthful or be fired – may be significantly curtailed, with the employee essentially having the right not to cooperate with little consequence.[88]

These dynamics may, of course, change if there is a parallel government investigation (which, as discussed below, creates its own issues), as the corporation may, in that instance, simply

[86] *France: Corporate Investigations 2020*, ICLG, https://iclg.com/practice-areas/corporate-investigations-laws-and-regulations/france.

[87] This may be seem counter-intuitive, but the point of *not* recording an interview relates back to the Federal Rules of Evidence. It is commonplace that a witness's recollection may change and hopefully improve over time. A recorded interview, however, freezes that recollection and, moreover, creates an "admission" that may be introduced in court against him. Although the interview may well be privileged, companies may often find it in their interest to produce such tapes as evidence of their own cooperation when employees refuse to sit for interviews with the government. In contrast to a tape, however, an attorney's notes of the interview are generally (albeit with some exceptions) viewed as privileged and covered by the work product protection and, more importantly, are the *attorney's* statement and not the witness's and thus, even if produced to the government, cannot be introduced into evidence in most instances.

[88] *France: Corporate Investigations 2020*, ICLG, https://iclg.com/practice-areas/corporate-investigations-laws-and-regulations/france. In France, for instance, employees are required cooperate with the internal investigation by delivering documents that are considered company property, but employees are not required to speak at an interview.

inform the prosecutor that a particular employee is not being cooperative, leaving that employee to the mercies of the prosecutor, who may not operate under the same constraints.

1. Clarity of Roles and Privilege Concerns

External counsel should consider the scope of representation and the lawyer-client relationship during interviews. An understanding of privilege is key to conducting a successful internal investigation. In the U.S., the scope of legal privilege covers the attorney-client privilege and attorney work product. Attorney-client privilege protects from the discovery of confidential communications between clients and their lawyers made for the purpose of obtaining or providing legal advice. Attorney work product protects from discovery documents and other materials prepared by a lawyer in anticipation of litigation. These topics can cover a diverse array of issues, but perhaps most critical in the course of an internal investigation is an understanding of who can provide the privilege.

Relatedly, under ABA Model Rules of Professional Conduct Rule 1.13, a "lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents."[89] Thus, when dealing with the company's "directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization's interests are adverse to those of the constituents with whom the lawyer is dealing."[90]

The need for this clarity arises in a number of situations. Under Model Rule 1.18, "[a] person who consults with a lawyer about the possibility of forming a client-lawyer relationship

[89] Model Rules of Prof'l Conduct R. 1.13 (2018).

[90] *Id.*

with respect to a matter is a prospective client."[91] As such, "[e]ven when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information, except as Rule 1.9 would permit with respect to information of a former client."[92] Thus, without a clear understanding between the lawyer and the witness as to whom the lawyer is representing, there is a risk that the information imparted to the lawyer under a potentially mistaken impression that the lawyer is representing both the company and the company's employee may be viewed as protected not only by the company's privilege but by the *witness*', thus empowering the witness to prevent the company from choosing to waiver its privilege and disclose that information even when it is in the company's interest.

Accordingly, under Model Rule 4.3, when communicating on behalf of a client with a person who is not represented by counsel, "a lawyer will typically need to identify the lawyer's client and, where necessary, explain that the client has interests opposed to those of the unrepresented person."[93] It is important to note, "[t]he Rule distinguishes between situations involving unrepresented persons whose interests may be adverse to those of the lawyer's client and those in which the person's interests are not in conflict with the client's. In the former situation, the possibility that the lawyer will compromise the unrepresented person's interests is so great that the Rule prohibits the giving of any advice, apart from the advice to obtain counsel." These rules are critical to running a successful interview process during an internal investigation as they emphasis the understanding that the "client" of an in-house attorney is the company.

---

[91] Model Rule of Prof'l Conduct R. 1.18 (2018).

[92] *Id.*

[93] Model Rule of Prof'l Conduct R. 4.3 (2018).

In most cases, lawyers conducting an investigation on behalf of a company will address these concerns and seek to ensure the witness is clear as to their role by giving the witness the so-called *Upjohn* warning.[94] The basic elements of an *Upjohn* warning include: (1) a declaration that the lawyer represents the company and not the individual employee; (2) the purpose of the interview is to gather information to provide legal advice for the company; (3) the conversation is privileged and confidential; (4) the privilege belongs to the company, and the company can waive it at any time and share with others (including regulators) information learned in the interview; (5) to maintain the privileged nature of the discussion, anything discussed must be kept confidential and not disclosed by the employee.

One key question, however, is the potential impact on the privilege if you are conducting the investigation *not* in connection with anticipated litigation or for the purposes of obtaining legal advice. In *United States ex rel. Barko v. Halliburton Co.*, the district court initially held that documents related to the company's internal investigation of an alleged scheme by the company and its subcontractors to accept kickbacks from military contracts in Iraq were not privileged and were instead business records because the investigation was "undertaken pursuant to regulatory law and corporate policy rather than for the purpose of obtaining legal advice."[95]

On appeal, the D.C. Circuit rejected that analysis, finding that it "rested on a false dichotomy. So long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, the attorney-client privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than

[94] Upjohn Co. v. United States, 449 U.S. 383 (1981).

[95] United States ex rel. Barko v. Halliburton Co., 37 F. Supp. 3d 1, 5 (D.D.C. 2014).

simply an exercise of company discretion."[96] Thus, "[i]n the context of an organization's internal investigation, if one of the significant purposes of the international investigation was to obtain or provide legal advice, the privilege will apply. That is true regardless of whether an internal investigation was conducted pursuant to a company compliance program required by statute or regulation, or was otherwise conducted pursuant to company policy."[97]

In the U.K., a communication sent to both lawyers and non-lawyers will be protected under the Legal Advice Privilege if the "dominant purpose" of the communication was to obtain legal advice.[98] However, material collected by a company, or its counsel, from third parties to instruct counsel is not protected, and communications between an employee and a company's counsel are only protected if the employee was told by the company to obtain legal advice from counsel.[99] Another key consideration is the difference between legal privilege in European Commission investigations as compared to privilege in the U.S. The EU Legal Professional Privilege (LPP) protects from discovery written communications between an external lawyer and his or her client that are sent for the purpose of the client's rights of defense in the Commission's investigation. Communications made for the client's "rights of defense" include: (i) those made after the initiation of an investigation or administrative procedure by the European Commission and (ii) preexisting written communications that are related to the subject matter of the European Commission's investigation or administrative procedure. Thus, legal advice given by an in-house

[96] In re Kellogg Brown & Root, Inc., 756 F.3d 758–59 (D.C. Cir. 2014) (Kavanaugh, J.).

[97] In re Kellogg Brown & Root, Inc., 756 F.3d at 760.

[98] *Court of Appeal Gives Important New guidance on Legal Advice Privilege*, SHEARMAN & STERLING (Jan. 31, 2020), https://www.shearman.com/perspectives/2020/01/court-of-appeal-gives-important-new-guidance-on-legal-advice-privilege.

[99] *Id.*

counsel in Europe can often be reviewed by the European Commission in competition law investigations.[100]

Other issues related to the clarity of the attorney's role may not be initially apparent but have significant consequences later. For example, in many cases, an internal investigation may be carried out under the eye of the government authorities, *e.g.*, where the company has met with the government and offered its cooperation. Here, there is a risk that the role of the company's attorney, both in terms of perception of the client, as well as in the eyes of the court, may be blurred. A client – or its employees – may question, for instance, whether the attorney is acting in the best interest of the corporation – or its employees – or for the benefit of the government and ask "where is the advocacy." It is important that the attorney explain clearly that there are phases to each representation, with the investigation stage necessarily being objective to ensure that the findings of the investigation, when presented to the government, are viewed as credible, thereby allowing them to form the basis of advocacy as to whether there has been a crime and, if so, what are the appropriate enforcement responses. If, to the contrary, the internal investigation is viewed as being limited in scope and its findings lacking objectivity and independence, the company is essentially inviting the government to conduct a much more disruptive and intrusive investigation, with concomitant greater costs and potentially more severe consequences.

It is, however, possible to go too far to the other side and, by taking direction from the government as to how to proceed with particular aspects of the investigation, to be viewed as having been co-opted by the government (or, from the other side, to have the government "outsource the investigation" to company counsel). As noted above, in *U.S. v. Connolly*,[101] the

[100] *See* Akzo Nobel Chemical Ltd and Akcros Chemical Ltd v European Commission, Case C-550/07 (CJEU).

[101] U.S. v. Connolly, et al., No. 16 CR 370 (S.D.N.Y May 2, 2019).

court found that the internal investigation, conducted in full view of the government, was essentially an extension of the government's investigation and the company's lawyers were acting at the direction of the government, resulting in the company's employees being entitled to certain constitutional rights, including those under the Fifth Amendment, during the company's interviews.[102]

2. Joint Defense Agreements

If the alleged misconduct implicates other companies, it may be worthwhile to consider whether the companies should enter into a joint defense agreement for as long as the companies' interests align. For example, a common interest may arise in the context of a merger and acquisition transaction in which both companies share an interest in determining the facts to manage and assign liability in connection with potential disclosure to the government or the market. However, when the companies are both potentially culpable (such as in an antitrust conspiracy), entering into a joint defense agreement may be problematic if it prevents the company for acting in its own interest. Similar issues may arise with respect to entering into a joint defense agreement between a company and individuals.[103]

---

[102] *Id.; See also* SEC v. Computer Association. International, Inc., No. 1:04-cv-04088 (E.D.N.Y. Oct. 1, 2004); SEC v. Kumar et al., No. 1:04-cv-04104 (E.D.N.Y. Oct. 1, 2007); SEC v. Woghin, No. 1:04-cv-4087 (E.D.N.Y. Dec. 29, 2009) (obstruction charges against the Computer Associates executives stemmed from statements they made to internal investigators which has led to the "*Zar*" warning ahead of internal investigation interviews noting that the information learned in an interview could or will be shared with an investigator).

[103] *See, e.g.*, United States v. Stein, 435 F. Supp. 2d 330 (S.D.N.Y. 2006) (holding the pressure put on the company by the prosecutors, who cited to the DOJ's Thompson Memorandum violated the individuals' Fifth and Sixth Amendment rights. The Thompson Memorandum outlined that the government could consider the extent of a

Joint defense agreements are governed by the common interest privilege, or joint defense privilege, which is related to the attorney-client privilege. That is, the common interest privilege allows parties who share common interests to share information without waiving the attorney-client privilege. The benefits of entering into a joint defense agreement include sharing costs and pooling resources and sharing information and coordinating strategy. While it is not necessary to enter into a formal agreement (an oral agreement is sufficient[104]), best practice may be for all parties involved to sign a document, the joint defense agreement, which outlines the parameters of the group's agreement. Many considerations can go into such an agreement but perhaps most important is to clearly describe that each party is represented only by its own counsel and to provide parameters for when a member of the group might cooperate with the government. Parameters for cooperation might include a notice period such that a member has to provide notice to the group before providing cooperation to the government.

3. Incentives

There are a number of reasons why employees may be reluctant to provide information during an investigation, including fear of retaliation by a supervisor or being implicated in the misconduct. Employers can encourage employees to cooperate with an investigation by offering them protection from termination if they come forward with information. One of the most well-known internal investigations of the past decade was the successful prosecution of Siemens AG by German and U.S. authorities for corruption offenses. For nearly two decades, Siemens conducted systemic bribery of public officials for multi-million dollar government contracts (*e.g.*,

company's cooperation if it was paying for individuals' counsel in a way that obstructed the government's investigation.).

[104] *See, e.g.*, Continental Oil Co. v. United States, 330 F.2d 347, 350 (9th Cir. 1964).

$340 million contract to build rail systems in Venezuela). The company was able to carry out and conceal the misconduct by using slush fund accounts, falsifying bookkeeping records, short-changing audits, and accumulating profit reserves as liability on the books, among other conduct.[105] Civil and criminal penalties across the U.S. and Germany totaled $1.6 billion.[106] However, one unique aspect of this investigation was Siemens' immense cooperation. According to the Acting Assistant Attorney General at the time, Matthew Friedrich, Siemens "faced facts, accepted responsibility, retained experienced counsel to conduct thorough internal investigations, and…implemented real reforms."[107]

One of the critical elements of the investigation involved two company-wide amnesty programs Siemens offered to employees. The programs were designed and implemented in consultation with German and U.S. authorities and resulted in over 100 employees providing relevant information to Siemens' external counsel. The first program gave all employees, aside from the most senior employees, protection from "unilateral employment termination and company claims for damages" for voluntarily disclosing "truthful and complete information about possible violations of relevant anti-corruption laws."[108] A second program was later offered for senior employees and lower-level employees who did not come forward during the first round. The second program provided "individualized leniency determinations for cooperating

[105] U.S. Dep't of Justice, Transcript of Press Conference Announcing Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations (Dec. 15, 2008), https://www.justice.gov/archive/opa/pr/2008/December/08-opa-1112.html.

[106] *Id.*

[107] *Id.*

[108] U.S. Dep't of Justice's Sentencing Memorandum, United States of America v. Siemens Aktiengesellschaft (D.D.C. Dec. 12, 2008), https://www.justice.gov/archive/opa/documents/siemens-sentencing-memo.pdf.

employees."[109] Not only did the program allow employees who had not shared information to come forward, it provided a safe avenue for employees who had withheld information or had been dishonest during earlier conversations to share information. Siemens communicated to employees that while the amnesty offered was not binding on any prosecutors or regulators, it would inform regulators of an employee's cooperation if he or she ever became the subject of an investigation. The amnesty program worked, in part, because German prosecutors had the ability to compel interviews of uncooperative employees, who could potentially face prosecution if they did not comply.

D. Wrapping up the Internal Investigation

After the initial findings have been formulated, the team running the investigation will often be asked to present its formal findings in a report or presentation to the Board or the Audit Committee. A report or presentation will typically provide an overview of the investigation methodology, describe what the investigation uncovered, identify any problematic behavior, polices, or specific individuals, and propose recommendation and remediation measures. Further, if the investigation uncovered clearly unlawful conduct, it is critical that such conduct be rooted out as early as possible.[110] This may entail disciplinary action, or revisions to the company's compliance programs or internal controls.[111]

If external counsel has taken the lead on the investigation, it should be cognizant of the possibility that disclosing unpleasant facts discovered during the internal investigation may result

[109] *Id.*

[110] Paula Anderson & Claudius Sokenu, *How a skilled board should manage an internal investigation*, DIRECTORS & BOARDS, (FIRST QUARTER 2015), at 36.

[111] *Id.*

in a negative reaction from the company. For instance, Eurasian Natural Resources Corporation (ENRC), a diversified natural resource group with mining operations, attempted to prevent its external counsel, Dechert, from disclosing its internal investigation findings to the U.K.'s Serious Fraud Office (SFO) during the SFO's investigation of the company.[112] ENRC brought a civil suit against Dechert, disputing a bill and claiming, among other things, that counsel went beyond the scope of the internal investigation, exaggerated findings, and breached its fiduciary duty to the company by disclosing information about the investigation to the SFO and the media.[113] Dechert maintained, however, that the investigation revealed evidence of fraud, corruption, and sanctions violations that warranted self-reporting the misconduct to the SFO (see Section III.A below on Self-Disclosure). Recently, a High Court in London ruled that the SFO's investigation cannot rely on documents from the ENRC civil case.[114] The ENRC case illustrates the importance of external counsel and in-house teams openly communicating during the investigation, managing the expectations of senior management after initial findings are formulated, and documenting findings.

III. Interacting with the Government and Responding to Government Investigations

Even if not required by law, a company should consider whether it is appropriate to voluntarily disclose the findings of an internal investigation to the public, often through public filings, or to government regulators. Voluntary disclosure carries with it risks and costs that may

[112] Richard Crump, *SFO Can't Use Docs From ENRC Civil Suit In Corruption Probe*, LAW360, May 7, 2020, https://www.law360.com/articles/1271258/sfo-can-t-use-docs-from-enrc-civil-suit-in-corruption-probe.

[113] Eurasian Natural Resources Corporation Ltd. v. Dechert LLP and others, case nos. CL-2017-000583 and CL-2019-000644 (U.K.).

[114] Richard Crump, *SFO Can't Use Docs From ENRC Civil Suit In Corruption Probe*, LAW360 (May 7, 2020), https://www.law360.com/articles/1271258/sfo-can-t-use-docs-from-enrc-civil-suit-in-corruption-probe.

be considerable, and thus whether to go down that road is a decision that must be made carefully. Although there are differing views (and the government obviously favors and provides incentives for voluntary disclosure), a company may justifiably conclude that a voluntary disclosure is only advisable, naturally, in cases where the investigation has uncovered a significant and substantive potential violation and, frankly, where there is a significant likelihood of disclosure by other parties or in those limited instances in which there is a legal obligation to do so.

A. Self-Disclosure

If a company decides to voluntarily disclose, timing is a critical consideration. For example, companies may wish to complete every step of an investigation with a goal to presenting the government with fully developed and conclusive findings. On the other hand, that takes time and presents various risks including that the government may learn of the allegations through other means or that the government will view the "delay" in making the disclosure as prejudicing its ability to conduct certain types of investigation (e.g., surveillance and wiretaps), to take wrongdoers into custody (because they were tipped off by the investigation), or to bring charges (because of the running of the statute of limitations). Even if the company was not intentionally hiding information from the agencies, this could lead to the DOJ characterizing the company's failure to disclose the information sooner as "unreasonably delaying reporting the offense," precluding the company from receiving deductions to its culpability score—an essential mechanism for fine reductions in criminal investigations.[115] Thus, although the DOJ encourages companies to conduct "a thorough review of the nature, extent, origins, and consequences of the

[115] *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, U.S. DEP'T OF JUSTICE CRIMINAL DIVISION & SEC ENFORCEMENT DIVISION (Nov. 14, 2012), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

misconduct," it also wants them to "promptly, completely, and effectively" disclose misconduct to regulatory agencies, the public, and internal compliance programs[116] and has strongly indicated that it views early disclosure of potential violations more favorably.

Factors to weigh when considering self-disclosure to government regulators may include: (1) whether there was indeed a violation; (2) whether the violation would typically be prosecuted by the government; and (3) the likelihood that the conduct would be discovered absent self-reporting. Factors the government would often consider are outlined in *Principles of Federal Prosecution of Business Organizations:* (1) nature and seriousness of offense; (2) pervasiveness of wrongdoing; (3) history of similar misconduct; (4) timely/voluntary disclosure and cooperation; (5) pre-existing compliance program's effectiveness; (6) remediation; and (7) collateral consequences.[117] Weighing these factors are critical because once conduct has been disclosed to regulators, the company has no control over what the government will do next.[118] However,

[116] *Id.* at 55.

[117] JM § 9-28.000, Principles of Federal Prosecution of Business Organizations, available at https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations. *See also* JM § 9-47.120, FCPA Corporate Enforcement Policy, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977 (which has been expanded to apply outside of the FCPA context); Memorandum from Mark Filip, Deputy Attorney General, U.S. Department of Justice, to Heads of Department Components and United States Attorneys (August 28, 2008) Memorandum from Sally Quillian Yates, Deputy Attorney General, U.S. Dep't of Justice, to All United States Attorneys (Sept. 9, 2015); and U.S. SENTENCING GUIDELINES MANUAL § 8 (2018).

[118] Paula Anderson & Claudius Sokenu, *How a skilled board should manage an internal investigation*, DIRECTORS & BOARDS (First Quarter 2015), at 36.

generally speaking, being open and forthcoming with the government will boost the credibility of the internal investigation.[119]

Aside from disclosing findings to government regulators, a company must also consider whether to disclose an investigation in SEC filings.[120] It is often the case that a company will try to coordinate the timing of a voluntary disclosure to government regulators with a disclosure in SEC filings.[121]

Further, once engaged with the government, companies will need to be able to persuasively present a picture of corporate commitment to compliance and a genuine effort to uncover and remediate wrongdoing. The DOJ in particular has demonstrated a growing sophistication in evaluating the effectiveness of corporate compliance programs. With respect to investigation, it will examine not just whether the investigation was thorough in scope but whether the company has taken on board the investigation's findings and identified and remediated root causes, system vulnerabilities, and accountability gaps as well as taking disciplinary actions against past bad actors.[122]

---

[119] *Id.*

[120] *Id.*

[121] *Id.* However, the SEC's Enforcement Division does not consider disclosure in a public filing to be a voluntary self-report.

[122] *Evaluation of Corporate Compliance Programs*, U.S. DEP'T OF JUSTICE CRIMINAL DIVISION (June 2020), at 16, 17, https://www.justice.gov/criminal-fraud/page/file/937501/download.

B. Privilege Waivers

The DOJ does not require a waiver of privilege for "cooperation credit."[123] However, there is still implicit pressure to voluntarily waive privilege. That is, there is still a need to disclose "relevant facts concerning…misconduct," including "factual information acquired through interviews."[124] In practice, the easiest way to comply with this requirement may be to share facts learned from witnesses, whether through outline, read-out, or delivery of interview memos. Further, the Yates Memo, published by the DOJ in 2015, emphasizes disclosure of "all relevant facts" and identifying culpable individuals further adds pressure to share details of witness interviews.[125] Similarly, the SEC may not request waiver "without prior approval of the Director or Deputy Director" of the Enforcement Division but, in practice, there is still pressure to voluntarily waive privilege.[126]

---

[123] *See* Memorandum from Mark Filip, Deputy Attorney General, U.S. Department of Justice, to Heads of Department Components and United States Attorneys (August 28, 2008). *See also* USAM § 9-28.700; *see also* USAM § 9-28.720 fn. 1 ("There are other dimensions of cooperation beyond the mere disclosure of facts, such as providing non-privileged documents and other evidence, making witnesses available for interviews, and assisting in the interpretation of complex business records.")

[124] Memorandum from Mark Filip, Deputy Attorney General, U.S. Department of Justice, to Heads of Department Components and United States Attorneys (August 28, 2008).

[125] JM § 9-28.700, The Value of Cooperation, available at https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.700.

[126] U.S. Securities and Exchange Commission Division of Enforcement, Enforcement Manual (Nov. 28, 2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

C. Coordination among Regulators in Different Countries

Increasingly, regulators across jurisdictions have joined forces in their investigation efforts. For example, in 2019, the DOJ and the UK Home Office introduced an agreement to permit law enforcement officials to obtain electronic data directly from companies who hold it in an effort to facilitate investigations of serious crimes by cutting down the time needed to access such data.[127] Further, Assistant Attorney General Makan Delrahim of the DOJ Antitrust Division expressed in 2019 that "[o]ver the past 25 years, it has become increasingly common for the Antitrust Division to coordinate closely with international enforcers. This cooperation benefits the enforcement agencies, the business community, and consumers, as we are able to share views of the evidence, expected timelines, and evaluations of potential remedies."[128]

1. Coordinated Resolution

There are a number of benefits to resolving various government investigations in a single, coordinated resolution. First, a coordinated resolution often means that all of the enforcement agencies will announce the resolution on the same day, resulting in "one-day" media coverage as opposed to coverage every time a resolution is reached with an individual enforcement agency. Second, a coordinated resolution is often preferable for stakeholders because they offer "finality." Third, if enforcement agencies work together toward a resolution, they are more likely to credit

[127] *FCPA Digest: Recent Trends and Patterns in the Enforcement of the Foreign Corrupt Practices Act*, SHEARMAN & STERLING LLP (Jan. 2020), https://www.shearman.com/ (search "FCPA Digest 2020").

[128] Makan Delrahim, Assistant Attorney General, "With a little Help from My Friends": Using Principles of Comity to Protect International Antitrust Achievements, Address at the 46th Annual Fordham Competition Law Institute Conference on International Antitrust Law and Policy (Sep. 12, 2019), https://www.justice.gov/ (search "Fordham Conference").

penalties among themselves. In fact, the DOJ has issued guidance to its attorneys on how to avoid "piling on" companies when coordinating enforcement actions with multiple agencies and jurisdictions. The Policy on Coordination of Corporate Resolutions encourages attorneys to "avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture" against a company for the same conduct.[129] Companies should try to ensure that settlements cover all jurisdictions where the alleged misconduct could be investigated and prosecuted and all charges related to the investigated conduct to prevent later enforcement in other jurisdictions. However, it must be noted that a coordinated response does not always work. For example, Siemens A.G. negotiated simultaneous settlements in the U.S. and Germany related to a bribery scheme.[130] However, Siemens then faced years of follow-on settlements in other countries, including Argentina.[131]

A properly run and credible internal investigation that results in appropriate remedial action may result in a better resolution with authorities. The DOJ in particular has a spectrum of possible resolutions ranging from guilty pleas resulting in a criminal conviction and potential collateral consequences, to Deferred and Non-Prosecution Agreements, in which the company admits facts, agrees to pay a financial penalty, and undertakes various compliance remediation and reporting obligations, to "declination with disgorgement," to outright declination. Obviously, although a

---

[129] Memorandum from Rod J. Rosenstein, Deputy Attorney General, U.S. Dep't of Justice, to All United States Attorneys (May 9, 2018), At 1, https://www.justice.gov/opa/speech/file/1061186/download.

[130] Siri Schubert & T. Christian Miller, *At Siemens, Bribery Was Just a Line Item*, N.Y. TIMES (Dec. 20, 2008), https://www.nytimes.com/ (search "Siemens Bribery").

[131] Gonzalo Vila, *In fallout from $*106 *million corruption scheme, Siemens managers face 'copycat' charges in Argentina,* ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS (Jan. 15, 2014), https://www.delitosfinancieros.org/in-fallout-from-106-million-corruption-scheme-siemens-managers-face-copycat-charges-in-argentina/.

declination is best, the other alternatives are favorable outcomes compared to criminal conviction through a guilty plea or trial. The DOJ may be more likely to agree to a NPA or DPA if the company has completed a thorough internal investigation and can demonstrate it has taken remedial measures. Similarly, when considering whether a monitor should be appointed, the DOJ considers whether "the corporation has made significant investments in, and improvements to, its corporate compliance program and internal control systems."[132] It is important to note that superficial changes to policies and procedures that fail to adequately address past misconduct will not suffice. The DOJ will consider whether the improvements "have been tested to demonstrate that they would prevent or detect similar misconduct in the future."[133]

Similarly, the SFO expects companies to adopt a "genuinely proactive approach" after learning of wrongdoing that includes cooperation with authorities. While the SFO has made it clear that cooperation does not guarantee a particular outcome, it has indicated that cooperation is a "relevant consideration" in its charging decisions, including the decision to offer a DPA.[134] Cooperation includes identifying suspected misconduct, identifying individuals involved in the misconduct, reporting to the SFO within a "reasonable time of the suspicions coming to light," preserving evidence, and promptly providing relevant evidence to the SFO.[135] In June 2020, France's Ministry of Justice issued guidance stating that companies are expected to cooperate with

[132] Memorandum from Brian A. Benczkowski, Assistant Attorney General, U.S. Dep't of Justice, to All Criminal Division Personnel (Oct. 11, 2018), At 2,DOJ, "Selection of Monitors in Criminal Division Matters," p. 2, https://www.justice.gov/opa/speech/file/1100531/download.

[133] *Id.*

[134] U.K. Serious Fraud Office, Corporate Co-operation Guidance, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/#.

[135] *Id.*

prosecutors to be eligible for the Public Interest Judicial Agreement (CJIP), a settlement agreement closely resembling deferred prosecution agreements.[136] Much like the cooperation requirements in the U.S. and U.K., companies in France are expected to share the names of the individuals involved in the misconduct with prosecutors.[137]

D. Collateral Business Consequences for Extraction Companies

There are various collateral business consequences that could arise as a result of the investigation. Generally, a company should be prepared for negative media coverage, civil litigation, and criminal charges against senior management and other key individuals.[138] For a mining company, specifically, collateral consequences may include limits on participating in public procurement or contracting with the government, temporary freezes or suspension of licenses and permits, and termination of contracts by third parties and vendors.

As previously mentioned, a coordinated resolution often results in "one-day" media coverage, meaning that the various regulatory authorities announce the resolution on the same day, reducing the amount of time the company stays in the news cycle. However, it should be noted that announcements by authorities may include unpleasant details about the investigation which will then be covered widely by media outlets. For instance, in an article published in Forbes, author Harry Broadman highlighted how corporate social responsibility and charitable donations were being used as a cover for bribery and corruption schemes to obtain government

---

[136] James Thomas, *France's Justice Ministry spurs on self-reporting*, GLOBAL INVESTIGATIONS REVIEW (June 11, 2020), https://globalinvestigationsreview.com/ (search "France self-reporting").

[137] *Id.*

[138] *See* Philip Urofsky, et al., *Civil Litigation in the Aftermath of FCPA and U.K. Bribery Act Investigations*, ANTI-CORRUPTION REPORT (May 13, 2020), https://www.shearman.com/ (search "Civil Litigation in the Aftermath of FCPA") (discussing civil litigations).

contracts. Broadman criticized the 2011 oil concession contract between BP, Cobalt, and Sonangol, where BP and Cobalt agreed to pay $350 million for the creation of the "Sonangol Research and Technology Center," a training site for Angolans to learn highly skilled aspects of natural resource extraction in order for them to work in and profit from extracting Angola's natural resources.[139] The site would have been run by Sonangol, Angola's state-owned oil monopoly.[140] BP and Cobalt made an initial installment payment of $175 million in 2011.[141] Broadman notes, "Remarkably, more than six years later there is no such center and no one seems to know where the money actually went."[142] Similarly, in 2017, the DOJ found that SQM, a Chilean chemical and mining company, paid $1 million to faux foundations at the request of Chilean officials with whom SQM did business.[143]

It is important that companies consider developing a communications plan that includes a clear narrative of events and answers to anticipated questions from the media before the press learns of investigations. It should be noted that responding to the media can be time-consuming,

---

[139] Harry Broadman, *When Too Much Corporate Social Responsibility (CSR) Is Too Good To Be True*, FORBES (May 30, 2018), https://www.forbes.com/ (search "too much corporate").

[140] Tim Fernholz, *The absence of a mysterious research center in Angola could be evidence of oil corruption*, QUARTZ (Aug. 12, 2014), https://qz.com/247521/the-absence-of-a-mysterious-research-center-in-angola-could-be-evidence-of-oil-corruption/.

[141] *Id.*

[142] Harry Broadman, *When Too Much Corporate Social Responsibility (CSR) Is Too Good To Be True*, FORBES (May 30, 2018), https://www.forbes.com/ (search "too much corporate"); Tim Fernholz, *The absence of a mysterious research center in Angola could be evidence of oil corruption*, QUARTZ (Aug. 12, 2014), https://qz.com/247521/the-absence-of-a-mysterious-research-center-in-angola-could-be-evidence-of-oil-corruption/.

[143] *Id.*

and if a company does not have an internal communications team equipped to develop a communications plan, it can request that external counsel handle media inquiries or it can hire a public relations firm. Companies will have to weigh the additional cost of hiring an external firm against the benefits of a cohesive narrative in the media and limiting bad press.

The press surrounding the announcement of the resolution may result in civil claims being brought against the company. In the U.S., it is common for shareholders to bring securities class actions against companies for losses allegedly suffered as a result of the company making a material misstatement or omission related to the misconduct.[144] Many such actions are brought in the form of shareholder derivative suits whereby the shareholders sue on behalf of the corporation against the officers and directors of the corporation to redress harm done to the corporation.[145] While such follow-on litigation is less common in the U.K., it is a possibility that shareholders, and in some case, competitors, sue the company alleging losses as a result of the misconduct.[146] Other regulatory authorities that were not involved in the coordinated investigation or resolution may decide to bring their own investigations. For instance, there is a possibility that foreign authorities that the company did not voluntarily disclose to could use disclosures in settlements with U.S. enforcement agencies to build a case against the company in foreign jurisdictions. Regulators in the "home country" of the company (*i.e.*, where the company is headquartered) may

[144] *See* Philip Urofsky, et al., Civil *Litigation in the Aftermath of FCPA and U.K. Bribery Act Investigations*, ANTI-CORRUPTION REPORT (May 13, 2020), at 1, https://www.shearman.com/ (search "Civil Litigation in the Aftermath of FCPA").

[145] *Id.* at 3.

[146] *Id.* at 6-7.

be pressured to prosecute a company even if the company already came to a resolution with the SEC or DOJ.

As discussed in Section II, directors and officers have duties of loyalty, care, and candor in the U.S., and if they fail to fulfill these duties, they could face claims of breach of fiduciary duty, corporate waste, and criminal charges for fraud. If convicted of FCPA-related violations, for instance, individuals could face up to 10 years in prison for serious misconduct and severe monetary fines. Individuals involved in the alleged misconduct may be terminated by their employer and face civil claims brought by the employer after termination. Additionally, the company may lose key personnel because of the investigation—either because the individuals no longer want to be associated with the company or because the company needs to hire new senior management or personnel as part of its remedial efforts. Odebrecht, as an example, was one of the companies involved in a scheme to create a slush fund from which bribes were paid out to Brazilian government officials. In December 2016, Odebrecht settled with U.S., Swiss, and Brazilian law enforcement authorities for $2.6 billion to resolve charges related to these schemes. The settlement documents outlined details of the company's wrongdoing and the company was required to disclose information about its activities as well as the activities of its subsidiaries. In 2019, the DOJ charged the former CEO of one of Odebrecht's subsidiaries for his role in the scheme. The former CEO was charged with conspiring to violate the FCPA's anti-bribery provisions, conspiring to violate the FCPA's books and records provisions, and conspiring to commit the FCPA's money laundering provision.[147]

[147] Press Release, U.S. Dep't of Justice, Former CEO of Braskem Indicted for His Role in Bribery Scheme (Nov. 20, 2019), https://www.justice.gov/usao-edny (search "Braskem").

In the U.S., the Federal Acquisition Regulations (FAR) allow for an individual or company guilty of violating the FCPA to be suspended or barred from government contracting. This action is based on the discretion of federal agencies, not the SEC or DOJ, and as such, guilty pleas, NPAs, and DPAs will not lead to automatic debarment.[148] An agency may, however, choose to suspend an individual or company based on an indictment alone. If an agency chooses to suspend or debar a contractor, then the suspension or disbarment applies to the entire federal executive branch unless an agency demonstrates compelling reasoning for not suspending or debarring the contractor.[149] When considering whether a company should become ineligible for government contracts, agencies often consider the effectiveness of a company's internal controls, whether the company voluntarily disclosed the misconduct in a timely manner, and whether the company has implemented remedial measures.[150]

Depending on the terms of the company's third-party and vendor contracts, the company may be obligated to notify third parties of the government's investigation and the subsequent resolution. There may also be termination rights that are trigged by the company's conduct and the outcome of the investigation. The company should consider creating an action plan for notifying its contractual counterparties of the outcome of the investigation and managing relationships with key vendors. The investigation may also trigger compliance-related covenants

[148] *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, U.S. DEP'T OF JUSTICE CRIMINAL DIVISION & SEC ENFORCEMENT DIVISION (Nov. 14, 2012), at 70, https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

[149] *Id.*

[150] *Id.*

in the company's credit agreements, requiring notification to the company's lenders and resulting in a possible event of default, and potential cross-defaults across the company's loan facilities.

IV. Conclusion

As illustrated above, several considerations need to be taken into account when addressing a whistleblower report. When a report is first received, the company will need to consider the incentives to come forward that the company and regulators offer individuals, and how whistleblowers could potentially use protection from retaliation as a shield or a sword. Investigating a whistleblower report and conducting an internal investigation may require navigating the laws of multiple countries in areas ranging from data protection and employment, to blocking statutes and attorney-client privilege. After an internal investigation concludes, the company may need to consider implementing remedial measures and decide whether it is appropriate to self-disclose potential misconduct. A government investigation carries with it important decisions regarding privilege waivers, cooperation with regulators, coordination among multiple regulators, and how to address collateral business consequences.

The bottom line is that a compliance officer's life is not easy. From the receipt of a whistleblower's report to the final conclusion, there are many significant and complex decisions that must be made, with many constituencies looking over your shoulder – the Board, the executives, data protection functions, employees, and, not least, the government!