CLEARY GOTTLIEB

Global Crisis Management Handbook

2018

Global Crisis Management Handbook

From your friends at Cleary Gottlieb

Introduction

What is Global Crisis Management?

Corporations operating in an increasingly globalized, regulated, and litigious environment must recognize that unexpected and potentially destabilizing events are, more than ever, likely to play out in the public eye and to elicit responses from regulators, criminal enforcement authorities, and private claimants across multiple jurisdictions. Such events can take a myriad of forms, from large-scale government investigations, to natural or man-made disasters (potentially resulting in harm to life and physical plant) to scandals involving senior executives. What differentiates such crises from more run-of-the-mill interactions with regulators, is their level of unpredictability, scope, and potential to cause harm to a business both from a legal perspective and by shaking the public's confidence in a business and its products. Such events call for a multi-disciplinary approach, including preparedness plans and coordinated legal and public relations strategy to address scrutiny from regulators, the press, and the public at once.

In the past, regulatory interest may have been cabined to events occurring in a physical jurisdiction or the home jurisdiction of a particular corporation. Now, however, with the increased speed and reach of news, regulatory competition, and public pressure to ensure that law enforcement and regulators are holding perceived bad actors to account, government agencies increasingly view their remit as increasingly globalized. Businesses operating across jurisdictions must therefore be prepared to respond in a coordinated way to requests from multiple government agencies located throughout the geographic areas their businesses touch. Moreover, given the increased speed and reach of the news cycle, businesses must be prepared to provide such a coordinated response in real time, frequently while the company itself is learning about the event, and as it plays out in public.

Recent decades have seen a substantial rise in the globalization of regulatory attention and law enforcement, exposing businesses to interest from regulators in multiple jurisdictions, often with competing processes, interests, and viewpoints. The reasons for this increased globalization of law enforcement are myriad, owing not just to the globalization of commerce. For example, in the wake of the 2008 Financial Crisis, regulatory and law enforcement agencies faced mounting political

and public pressure to bring significant cases and to demonstrate a willingness to bring corporate wrongdoers to account. In addition, the ever-increasing speed with which information is shared through the world has made it less likely that the effects of news events—including those involving corporations—remain in a company's home jurisdiction or the locale where the event occurred. Moreover, it cannot be excluded that local, or nationalistic, politics within a particular jurisdiction today may subject a business to intense regulatory and criminal scrutiny for conduct that once might have been investigated—if at all—through civil processes.

What is the purpose of this Handbook?

Addressing a global crisis event requires not just a recognition that speed, coordination, and cross-border functionality are essential, but also that a coordinated and multi-disciplinary approach is best suited to see a corporation through the myriad, and sometimes competing, issues presented by large-scale events. Responding to cross-border regulatory inquiries requires sensitivity to the local issues in connection with law enforcement authorities in every one of multiple separate jurisdictions. However, it is also essential that a business that is subject to a cross-border regulatory inquiry adopt a coordinated, and frequently uniform approach to issues that cut across jurisdictions. These can run the gamut from how to conduct internal investigations and implement remediation, to how to address corporate governance concerns, to how to prepare for potential follow-on litigations. All the while a business subject to a global crisis must be sensitive in how to appropriately communicate with relevant stakeholders, such as external auditors and shareholders, and the media.

This Handbook is designed as an introduction to thinking about the many legal and practical implications that frequently arise in cross-border investigations or other large-scale corporate events. It is not meant as a "how to," but rather as a "go-to"—the starting point for thinking about some of the issues routinely presented by such events. We have designed this as a desk reference to help you spot issues and avoid common mistakes, particularly at the outset of a crisis or investigation. This Handbook is not intended to provide, and should not be relied on as, legal advice. Rather, it is intended to serve as a starting point regarding how to handle a particular issue, which requires a sensitive, particularized, and nuanced understanding of the facts and the regulatory imperatives of the investigating jurisdictions arising from the specific matter. While it addresses the law in a variety of jurisdictions, this initial edition emphasizes U.S. legal concepts and cross-border issues by

comparison with those concepts in light of the prominent role U.S. authorities and courts take in such matters.

This Handbook is divided into nine chapters, each focused on an area of concern common to cross-border investigations, including:

— Considerations relevant to quickly understanding the facts of a matter, and managing public perception. (Chapter I: Managing the First Response, Chapter III: Conducting an Internal Investigation, Chapter VIII: Public Relations & Message Management).

— Considerations relevant to appropriately and efficiently working to address concerns of governmental authorities. (Chapter II: Responding to Requests from Authorities, Chapter VII: Cooperation).

— Legal issues that typically arise during investigations, particularly those presented by differing legal regimes. (Chapter IV: Preserving Legal Privilege, Chapter V: Data Privacy & Blocking Statutes, Chapter VI: Employee Rights and Privileges).

— Possible collateral consequences associated with large-scale governmental investigations. (Chapter IX: Collateral Considerations).

Throughout the Handbook, we have included practical guidance set out in color-coded boxes for ease of reference, meant to provide easy-to-use summaries of the various relevant legal regimes and practices, as well as the application of the topics of each chapter to real-world events.

— Blue: "Practice tips" to help you quickly identify many of the themes common to cross-border inquiries.

— Yellow: "Case studies" examine what has, and what has not, worked in past events.

— Green: "Elements" provide summaries of particular legal or regulatory requirements.

— Grey: "Government practice" summarizes practices and policies of various criminal or regulatory authorities.

The Handbook also contains helpful checklists keyed to particular phases of crisis management and incident response. They are cross-referenced against the substantive portions of the Handbook, and designed to help you quickly think through and identify information that may be necessary for the task at hand.

Of course every crisis is unique, presenting different factual and legal issues. And, given the number of jurisdictions in the increasingly-globalized regulatory landscape, it is not possible in a summary fashion to address them all. Our goal is, thus, not to provide a comprehensive survey of legal regimes or, indeed, to describe in any detail the differing approaches taken by myriad regulatory agencies. Instead, we hope this Handbook will introduce you to some of the competing interests in managing a global regulatory crisis, provide some useful insight into issues common to such events as well as practical steps for thinking about how to address them.

Table of Contents

Chapter I: Managing The First Response

Summary

How a "Global Crisis" Can Begin

— ***Regulatory Action:*** A regulatory or law enforcement authority may initiate an investigation through either a compulsory or voluntary request for information, or a dawn raid.

— ***Internal Escalation:*** An issue may be escalated internally, for example, by a whistleblower, concerned employee, or auditor.

— ***Public Media:*** An issue may be reported in public media, alerting members of a particular industry that an investigation is likely forthcoming, if not already underway.

— ***Triggering Event:*** A crisis may occur from a triggering event such as, for example, a data breach, cyber-attack, harassment scandal, or environmental disaster.

Creating a Plan of Action

— ***Preserving Legal Privilege:*** Legal counsel should be involved as early as practicable to avoid an inadvertent privilege waiver.

— ***Defining the Issue(s):*** Potential issues should be identified and defined as early as possible in order to determine the focus and scope of an investigation, build a response team, and notify any necessary stakeholders.

— ***Assessing Risks:*** Assessing the risks of liability that a company and its employees could potentially face will assist in navigating the first response.

— ***Conducting an Internal Investigation:*** Preserving evidence and crafting a protocol for information gathering and review early on will facilitate the investigation's progress and aid in crisis management.

— ***Adapting the Approach:*** Maintaining flexibility to adapt the approach as necessary is crucial to address any new issues that may arise as an investigation progresses or a crisis otherwise unfolds.

— ***Preparation is key:*** Incident response plans, as well as strong compliance and training programs, can be instrumental in managing the first response.

Introduction

A "global crisis"—the subject of this Handbook—can begin in a variety of ways. While some crises are more amenable to a predetermined plan of action than others, certain steps can be taken by a company as part of its first response to help manage the crisis and the progression of any subsequent investigation. This chapter explores some of the ways a global crisis can start, as well as relevant considerations for effectively managing the first response, so that a company is best positioned to respond swiftly and avoid potential missteps as the crisis unfolds.

How can a Global Crisis begin?

The most straightforward example of how a crisis can begin is a request for information from a government or law enforcement authority, particularly where multiple jurisdictions and authorities might be involved.[1] In some instances, an authority may execute a dawn raid or, in the United States, a search warrant, seizing documents and interviewing employees on the spot about possible misconduct. Often the action by authorities becomes public very quickly, in the form of news reports about the request, or pictures and reports from regulatory action.

Absent government action, a crisis may occur internally or be triggered by an external event. For example, a crisis may occur through an escalation by a whistleblower, concerned employee, or auditor. Alternatively, a company may be alerted to a potential crisis through external media reports, such as allegations in a newspaper article or online posting.[2] Similarly, a triggering event, such as a cyberattack,[3] allegations of

[1] Responding to requests from authorities is discussed in further detail in Chapter II: Responding to Requests From Authorities.

[2] For example, in 2008, *The Wall Street Journal* published an article suggesting that certain banks may have misrepresented their financial position and casting doubt on the legitimacy of the London Interbank Offered Rate ("LIBOR"). Carrick Mollenkamp, *Bankers Cast Doubt On Key Rate Amid Crisis*, Wall St. J. (Apr. 16, 2008), https://www.wsj.com/articles/SB120831164167818299. Government investigations in various jurisdictions commenced in the wake of that article, leading to an industry-wide, global investigation of LIBOR and other benchmark rates.

[3] For example, the 2017 Equifax data breach exposed sensitive personal information of approximately 145 million people in the U.S. In the wake of the breach, Equifax became the subject of multiple government investigations. Stacy Cowley, *Equifax Faces Mounting Costs and Investigations From Breach*, N.Y. Times (Nov. 9, 2017), https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html.

harassment,[4] or an environmental disaster,5 may cause both immediate financial and reputational harm to a company (and even harm to individuals) that can quickly spread through media reports and follow-up inquiries from authorities around the world.

Where an issue arises through channels other than a regulatory or government request for information, a company may have the opportunity to get a head start in determining its next steps without input from external authorities or pressure from the media and public reaction, even if a regulatory or law enforcement investigation ultimately ensues.[6] Further, even where a company is first alerted to a crisis through a request for information, its initial response will nonetheless help guide the progression of the ensuing investigation.

Assessing and Managing the Crisis

Regardless of how a potential crisis starts, identifying and defining the issues and forming a well-crafted plan of action early on is critical, and may become increasingly significant as an investigation progresses. Issues overlooked in the early phases of an investigation could prove very costly down the road, limiting options or potentially subjecting a company to greater penalties. Thus, a carefully crafted plan for managing the first response should consider the scope of the crisis and focus of an investigation, the methods for conducting the investigation and necessary resources, and the potential outcomes and impact on the company.

[4] For example, in 2017, a former Uber engineer stated in a blog post that she had been sexually harassed by her supervisor while employed at Uber, prompting Uber to initiate an internal investigation with the assistance of external counsel, and to terminate the employment of twenty employees following the investigation. Mike Isaac, *Uber Fires 20 Amid Investigation Into Workplace Culture*, N.Y. Times (June 6, 2017), https://www.nytimes.com/2017/06/06/technology/uber-fired.html.

[5] For example, in 2015, a dam operated by Brazilian mining company Samarco Mineração S.A. collapsed, killing nineteen people and devastating communities. The incident led to a ten-month investigation and significant financial penalties for the owners of the mine. The Fundão Tailings Dam Investigation, http://fundaoinvestigation.com/ (last visited Aug. 21, 2018). Dom Phillips, *Samarco Dam Collapse: One Year On from Brazil's Worst Environmental Disaster*, The Guardian (Oct. 15, 2016), https://www.theguardian.com/sustainable-business/2016/oct/15/samarco-dam-collapse-brazil-worst-environmental-disaster-bhp-billiton-vale-mining..

[6] In addition, as discussed further in Chapter VII: Cooperation, responding promptly to an internal escalation may allow a company to obtain cooperation credit with an investigating authority, which may, in turn, enable a company to mitigate any potential sanctions in connection with a settlement.

CAUTIONARY TALE:
$2.3 BILLION DOJ SETTLEMENT INITIATED BY WHISTLEBLOWER LAWSUITS

Although a whistleblower may present a company with the opportunity to address an issue internally, he or she may also escalate the issue to a regulatory or law enforcement authority or initiate a private suit where authorized by law. For example, in 2009, Pfizer was fined $2.3 billion in a settlement with the Department of Justice ("DOJ") to resolve criminal and civil liability for illegally promoting certain pharmaceutical products, and its subsidiary pled guilty to a federal crime. The DOJ's settlement announcement noted that its investigation was triggered by whistleblower lawsuits filed by former employees under the *qui tam* provisions of the False Claims Act ("FCA"),[7] and that the whistleblowers would receive payments totaling over $102 million from the federal share of the civil recovery as part of the settlement.[8]

Preserving Privilege

As a critical first step in responding to any crisis, a company should undertake to preserve legal privilege by involving counsel. Doing so will ensure that, among other things, a company's discussions about responding to the crisis, as well as the investigative steps and findings of the investigative team, will be protected from disclosure to third parties. Regardless of whether the company will rely solely on its in-house counsel or retain outside lawyers to manage and respond to a crisis, a company's legal department should be contacted as early as practicable to advise on initial steps and, most importantly, to ensure that legal privilege is not inadvertently waived.[9] (In some jurisdictions, of course, communications with in-house counsel do not have the same privilege protections as if external counsel is involved, so it is also important to consider local privileges laws). If outside counsel is retained, the

[7] Under the *qui tam* provision of the FCA, private individuals can file suit for violations on behalf of the government, which the government will subsequently investigate and determine whether to intervene in the suit. *See* 31 U.S.C. § 3730 (2018).

[8] Gardiner Harris, *Pfizer Pays $2.3 Billion to Settle Marketing Case*, N.Y. Times, (Sept. 2, 2009), http://www.nytimes.com/2009/09/03/business/03health.html; Press Release, Dep't of Just., *Justice Department Announces Largest Health Care Fraud Settlement in Its History* (Sept. 2, 2009), https://www.justice.gov/opa/pr/justice-department-announces-largest-health-care-fraud-settlement-its-history.

[9] Note that unlike the attorney-client privilege, "the work product privilege is not automatically waived by any disclosure to a third party." *See In re Sealed Case*, 676 F.2d 793, 809 (D.C. Cir. 1982). For a waiver to occur, the work product must be disclosed to an adversary, or create a risk that the documents will be disclosed to an adversary. *See In re Steinhardt Partners L.P.*, 9 F.3d 230, 235 (2d Cir. 1993); *Brown v. NCL (Bahamas), Ltd.*, 155 F. Supp. 3d 1335, 1339 (S.D. Fla. 2015). Though courts are not unanimous, the majority rule holds that independent auditors are not inherently adversarial to the companies they audit, and thus disclosure to outside auditors does not waive the work product protection. *See, e.g., United States v. Deloitte LLP*, 610 F.3d 129, 140 (D.C. Cir. 2010).

company's legal department should generally be kept fully informed and consulted throughout the company's response, including in an investigation.[10] In addition, it is generally advisable to involve either in-house or outside counsel in informing other internal stakeholders and external parties of the crisis to preserve legal privilege, and to ensure that those internal stakeholders involve lawyers in their discussions of any response, to protect the privilege.

Determining the Scope of the Problem

In addition to involving and retaining legal counsel, defining the potential scope of a crisis is an essential early step in formulating an effective plan of action. If a regulatory or law enforcement request has been received (or if a dawn raid was executed), the requesting or executing authority may provide some guidance regarding the investigation's focus that provides a starting point for the investigation. Even with such guidance, however, the requests may be broad and will likely require further scoping through discussions with the investigating authority and/or an internal investigation.[11]

If an issue arises in the absence of an external request, the focus of a potential investigation may be murky at the outset and require further scoping by the company. In such cases, a company may consider conducting a preliminary investigation, including informal scoping interviews or a limited document review to hone in on the key issues and guide a further investigation. If regulatory or law enforcement authorities are not yet involved, a company should consider the likelihood that they will investigate, such as, for example, if peer institutions are already under investigation.

It bears mention that certain legal obligations could necessitate an investigation irrespective of the involvement of investigating authorities. For example, a company's board of directors may have an obligation to conduct an investigation in order

[10] Different considerations relating to in-house counsel may apply to the extent that a special committee of the Board is conducting an investigation, and external counsel is representing the Board or Board committee in connection with the matter.

[11] *See* Chapter II: Responding to Requests from Authorities for further discussion regarding responding to regulatory requests.

to satisfy its fiduciary duties and to mitigate any consequences related to alleged misconduct.[12]

Assessing Risks and Potential Liability

Although the consequences of a crisis cannot be predicted with certainty, assessing a company's potential liability may guide its first response and frame the forthcoming investigation. In addition, identifying the potential penalties may help develop the company's plan of action through consideration of how such penalties can potentially be mitigated (e.g., through cooperation or remediation of any wrongdoing), and whether it is sensible to set aside reserves for potential fines and other expenses associated with an investigation. The severity of such penalties may also shed light on who needs to be informed, including for example, whether any public disclosures will be necessary.

Civil or criminal enforcement liability

In a civil enforcement action, a company may be subject to monetary penalties, and potentially suspension from certain business activities. In addition, a company may be ordered to engage in specified remediation efforts as part of a settlement. In the case of a criminal investigation, there are a range of possible outcomes, including the filing of a criminal charge, to which the company may be required to plead guilty, a deferred prosecution agreement ("DPA"), in which prosecution of the company is deferred for a period of time while the company engages in remediation and demonstrates good behavior, or a non-prosecution agreements ("NPA"), in which the DOJ decides not to prosecute the company. A criminal conviction, and even a DPA or NPA, can have a significant financial and reputational impact, including, for example, debarment, revocation of certain licenses, or the imposition of a monitorship.

[12] *See In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996) (holding that directors must implement a corporate program to identify potential wrongdoing in order to meet their duty of oversight); *see also Stone v. Ritter*, 911 A.2d 362 (Del. 2006) (confirming the *Caremark* standard and adding that directors must exercise "good faith" in dealing with potential or actual violations of law or corporate policy).

Private civil litigation

In addition to liability in the enforcement context, a company may also be named by private plaintiffs in civil litigation arising from the events of the crisis. For example, class action lawsuits in the United States are often filed once a significant government investigation is announced, particularly where that investigation results in a significant drop in the stock price of the company. Such lawsuits may proceed in parallel or be stayed pending the outcome of a government investigation. Plaintiffs in such suits are likely to capitalize on information that becomes public through the investigation, and may potentially seek information produced to investigating authorities as evidence, thereby illustrating one of the many reasons that preserving legal privilege from the start is critical.[13]

Individual liability

A company may seek to determine whether any individuals, such as employees, officers, or directors, may be subject to liability. Because a company can be held liable for the acts of its employees,[14] reaching this determination as early as possible may help frame the investigation plan and permit the company to promptly address wrongdoing by employees by taking disciplinary action where appropriate. In addition, where there is potential for individual liability, a company may consider retaining individual counsel to avoid any actual or apparent conflicts of interest. Certain employees, as well as officers and directors, may also be covered by indemnification provisions, either in their employment contracts or through the operation of the company's bylaws, through which the company may be responsible for the advancement or indemnification of an individual's legal fees or certain settlement expenses.[15]

[13] Follow-on civil litigation is discussed in further detail in Chapter IX: Collateral Considerations.

[14] Corporate criminal liability has traditionally been imputed to the company when an employee commits a crime while acting in the scope if his or her employment, at least in part for the benefit of the company. *See New York Cent. & Hudson River R.R. Co. v. United States*, 212 U.S. 481, 494-95 (1909); *United States v. Ingredient Tech. Corp.*, 698 F.2d 88, 99 (2d Cir. 1983), *cert. denied*, 462 U.S. 1131 (1983) (finding that the "acts of individuals on [the company's] behalf may be properly chargeable to it."); *United States v. Singh*, 518 F.3d 236, 250 (4th Cir. 2008) ("[A] corporation accused is liable for the criminal acts of its employees and agents acting within the scope of their employment for the benefit of the corporation, and such liability arises if the employee or agent acted for his own benefit as well as that of his employer.") (internal quotations and citations omitted).

[15] Issues regarding employees are discussed in further detail in Chapter VI: Employee Rights and Privileges.

Collateral consequences

Finally, a company may also consider the potential for collateral consequences arising out of the resolution of a crisis, which could negatively impact the company and/or its employees. For example, a company may be disqualified from certain regulatory statuses or exemptions as a consequence of civil administrative orders or criminal convictions, which may have broader implications for the company's ability to conduct its business.[16]

ASSESSING POTENTIAL LIABILITY: QUESTIONS TO ASK

- What is the scope of potential civil or criminal liability?
  - What is the nature of the conduct at issue?
  - Who are the investigating authorities (i.e., regulatory or law enforcement), if any?
  - What are the potential sanctions?
  - Who are the potential private plaintiffs?
- Is there potential for individual liability?
  - Can the company be found liable for the actions of individual employees?
  - Is any disciplinary action appropriate?
  - Should the company retain counsel for any individuals?
- Are there any collateral consequences to consider?

Notifying the Necessary Parties

In addition to identifying and scoping the issue, a company should consider as part of any immediate response whether any internal or external parties need to be notified, as well as the appropriate time to do so. A company may be legally obligated to notify certain parties promptly, whereas notifying other parties may risk waiving privilege.

[16] Collateral considerations are discussed in further detail in Chapter IX: Collateral Considerations.

Board of directors and management

It is critical to keep the board of directors and senior management informed of key developments relating to a possible crisis.[17] In certain circumstances, lawyers may be legally obligated to escalate issues to management. Similarly, if either internal or external auditors identify an issue, they may be required to inform "the appropriate level of the management" of the company, including either the board of directors or an appropriate special committee.[18] Additionally, as discussed below, a company should consider whether the investigation raises any potential conflicts of interest between the company and any officers or directors, which might require the formation of a special committee to oversee the investigation.[19]

Human resources and compliance

It may be helpful to involve a company's human resources and compliance departments in the event that issues arise with respect to particular employees and their conduct. Compliance, in particularly, plays an important role as the so-called "second line of defense," and in designing policies and procedures designed to prevent and detect misconduct. It will also be critical to consult with these departments before any disciplinary action is taken.[20]

Regulatory and law enforcement authorities

In cases where misconduct is uncovered or suspected before a law enforcement or regulatory inquiry, a company will need to determine whether, and if so, when to self-report the issue. The company may be legally obligated to self-report by statute, regulation, or under an existing agreement with the investigating authority, such as a DPA.[21] Even if self-reporting is not obligatory, there may be benefits to doing so, such as the potential to obtain cooperation credit with the authorities, to exercise

---

[17] *See Stone v. Ritter*, 911 A.2d at 365 (Del. 2006) (adopting liability standard for directors from *In re Caremark Int'l Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996)); 15 U.S.C. § 78m (b)(6) (2018) (requiring publicly held companies to "devise and maintain a system of internal accounting controls" to guarantee accurate financial statements and guard against misappropriation of assets).

[18] *See* 15 U.S.C. § 78j-1(b)(1) (2018).

[19] *See, e.g., Weinberger v. UOP, Inc.*, 457 A.2d 701, 709 n.7 (Del. 1983) (noting that forming an independent committee to consider a proposal would have been an indication of arms-length dealing); *see also Cede & Co. v. Technicolor, Inc.*, 634 A.2d 345, 361 (Del. 1993), *modified*, 636 A.2d 956 (Del. 1994) ("[T]he duty of loyalty mandates that the best interest of the corporation and its shareholders takes precedence over any interest possessed by a director, officer or controlling shareholder and not shared by the stockholders generally.").

[20] Employee rights and privileges are discussed in further detail in Chapter VI: Employee Rights and Privileges.

[21] *See, e.g.*, 41 U.S.C. § 8703(c) (2018) (requiring companies that do business with the federal government to disclose any reasonable grounds to believe that kickbacks were paid); 12 C.F.R. § 21.11 (2018) (requiring federally insured banks to submit Suspicious Activity Reports if they believe they have been defrauded). For an example of a DPA requiring ongoing cooperation and reporting, *see* Dep't of Just., *Deferred Prosecution Agreement*, https://www.justice.gov/usao-nj/file/829701/download.

greater control over any ensuing investigation, and ultimately, to receive a lower penalty if the authorities decide to take action.[22] At the same time, however, the company may want to consider the risks of premature notification.

With respect to timing, it may be in the company's best interest to report an issue as early as possible and before authorities learn about it from another source, particularly if the problem appears to be a serious one and is substantiated. For example, under the DOJ's Corporate Enforcement Policy, self-reporting before the DOJ becomes aware of wrongdoing can, absent aggravating circumstances, makes a company eligible for a declination or a substantial reduction of 50 percent off of a possible penalty.[23] A company will need to balance the benefits of quickly self-reporting against the need to familiarize itself with the facts and potential consequences before approaching a regulatory or law enforcement authority. In addition, a company may first seek to ensure that all necessary sign-offs have been received internally, in particular by the board of directors and management, before making any disclosures. A company should also keep in mind that disclosures made while cooperating with a regulatory or law enforcement authority may waive privilege, and consider ways to protect it.[24]

External auditors

A company may need to update and manage its external auditors during the course of a crisis or investigation. It is important to note, however, that disclosure of privileged information to an external auditor may waive privilege, so while managing the potential concerns of external auditors is critical, it should also be done in a way that best protects the company's privilege over the investigation and its findings.

Public disclosure

There may be situations in which a company chooses, or is legally required, to make a public statement or formal disclosure of an investigation.[25] For example, in the event of a crisis, such as an already public natural disaster or data breach, the company may wish to issue a press statement in an effort to address media reports or public concerns. Additionally, in some circumstances, public companies may be

[22] Considerations regarding self-reporting are discussed in the context of cooperation in Chapter VII: Cooperation.

[23] The Corporate Enforcement Policy is discussed in further detail in the context of cooperation in Chapter VII: Cooperation.

[24] Considerations regarding privilege are discussed in further detail in Chapter IV: Preserving Legal Privilege.

[25] Public relations issues are discussed in further detail in Chapter VIII: Public Relations & Message Management.

obligated under local securities laws to report a pending investigation as a material fact that must be disclosed, either immediately or in subsequent securities filings.

The First Response

CHECKLIST:
CREATING A PLAN OF ACTION

- ✓ Establish a response team
- ✓ Preserve and gather any relevant evidence
- ✓ Conduct a preliminary investigation
- ✓ Maintain a record and determine next steps

Building a Response Team

In the face of a crisis, a company should create a team of key stakeholders to lead the initial response. Identifying who will serve on the response team early on will encourage accountability, ensure that appropriate perspective and key stakeholders are included and can assist with preserving privilege, estimating and preparing for the costs associated with the investigation, and predicting other relevant issues that may arise. A response team will often be drawn from the following groups:

Legal counsel

As discussed above, involving legal counsel, whether in-house counsel or outside counsel, is critical to preserving legal privilege at the outset of an investigation. In addition, it is best to determine early on whether to retain outside counsel, so that any retained counsel is up to speed from the beginning. Circumstances that may favor hiring outside counsel include the complexity of the factual and legal issues, the scope of the investigation, and whether the company is simultaneously involved in any other investigations.

In addition to the logistical considerations, outside counsel may offer expertise in the particular factual or legal subject matter that is implicated in the investigation. If regulatory and/or law enforcement authorities are involved, retaining

outside counsel who are familiar with such authorities and investigations may be helpful in both anticipating and addressing issues. Further, outside counsel can provide credibility to an investigation because they are not part of the company, and can demonstrate that the company is taking the issue seriously. This is especially relevant if the company suspects involvement of senior management in the problematic conduct, such that in-house counsel may face a potential conflict of interest. Further, the company should consider hiring outside counsel to protect the privilege in jurisdictions where in-house counsel is not afforded the same level of privilege protection.[26] Finally, where an issue may have implications in other jurisdictions—for example, where a company has international offices—it may be necessary to involve local counsel to represent the company or, at minimum, advise on the particular laws of that jurisdiction.

As discussed above, even when outside counsel is retained, a member of the company's legal department should be kept involved as part of the response team to serve as an internal point person for the first response and any subsequent investigation.

Forming a special committee

If a conflict of interest arises, or is likely to arise, within the board of directors or management, such as specific allegations against a CEO or board member, a company should consider whether a special committee might be necessary to oversee the investigation.[27] If the company decides to create a special committee of the board of directors, privilege concerns will likely require walling off senior management or certain members of senior management because committees may not share the company's privilege.[28] In addition, special committee meeting minutes should also be kept separate from those of the regular board minutes to ensure that privilege is maintained. Moreover, the special committee should consider engaging its own counsel to ensure the independence of the investigation (rather than use regular company counsel).

---

[26] Preserving legal privilege is discussed in further detail in Chapter IV: Preserving Legal Privilege.

[27] *See supra* note 20.

[28] In *Moore Bus. Forms, Inc. v. Cordant Holdings Corp.*, the court noted that a special committee of the board could have hired its own lawyer to represent just the committee, which would have allowed them to withhold privileged communications from other members of the board. Nos. 13911, 14595, 1996 WL 307444, at *6 (Del. Ch. June 4, 1996); *see also Ryan v. Gifford*, No. 2213-CC, 2007 WL 4259557, at *3 (Del. Ch. Nov. 30, 2007) (holding that attorney-client privilege was waived where a special committee report was shared with implicated members of the board and their personal counsel).

Business personnel

Depending on the nature of the crisis, there may be certain individuals within the business who will need to be informed, involved in the response, and updated as the response proceeds.

Public Relations

Because the company may need a strategy for responding to requests for comment from the media, or affirmatively issuing its own statement to address a crisis, the company's public relations function should consult with the response team while taking care to ensure that such consultations do not result in waiver of the privilege.

Experts

In addition to legal counsel, other outside professionals may be helpful in facilitating an investigation, such as, for example, auditors, forensics specialists, subject-matter experts, data processing or document review services, or data analysis specialists. Such experts may be retained by counsel to facilitate the provision of legal advice, in which case their work would be protected by the attorney-client privilege.[29]

Preserving the Evidence

In the wake of a crisis, a company should take appropriate steps to preserve evidence and prevent spoliation. If the company faces a reasonable anticipation of litigation, a preservation notice should be sent to the relevant personnel, explaining the need to preserve documents and data. A company should take care in how it describes the materials that need to be preserved. Ordinarily, all relevant documents, including communications, data, and other documents stored on company-issued devices, should also be preserved, and routine deletion protocols should be suspended. A company may consider applying the same preservation efforts to personal devices, which are becoming increasingly pertinent when they might contain information potentially relevant to an investigation.[30] Failure to preserve evidence not only hinders the investigation but may also expose the company to potential sanctions or liability. Thus, a company should keep a clear record of all measures taken to preserve documents and information, including compliance certifications from

[29] *See United States v. Kovel*, 296 F.2d 918, 921 (2d Cir. 1961).

[30] *See, e.g., Brown Jordan Int'l, Inc. v. Carmicle*, No. 0:14 Civ. 60629, 2016 WL 815827 (S.D. Fla. Mar. 2, 2016) (finding severe sanctions under Rule 37(e)(2) for failing to preserve potentially relevant communications from personal devices).

those who received a preservation notice. This record will be useful if questions later arise about the company's preservation efforts.

Finally, while every company should have a document retention policy in place, following an existing document retention policy does not excuse a failure to act to preserve data once there is notice of impending litigation.[31] On the other hand, failing to follow the company's existing policy (and destroying document in a manner inconsistent with that policy) may weigh against a destroying party.[32] In addition, there may be statutory obligations requiring a company to retain certain documents, irrespective of its specific retention policy.[33]

Information Gathering and Review

As discussed above, before beginning a full-fledged internal investigation, a company may choose to conduct a preliminary investigation through a limited collection and review of documents and information, which may include the following:

Document review

A company might first seek to identify any categories of documents that are most likely to contain relevant information, limiting searches by using date ranges and identifying relevant custodians. The company might then commence a limited document review, guided by review protocols that explain the purpose of the review and relevant procedures.

---

[31] S*ee, e.g., Pillay v. Millard Refrigerated Servs., Inc.*, 09 Civ. 5725, 2013 WL 2251727, at *3 (N.D. Ill. May 22, 2013) ("As general counsel, Mr. Offner is charged with knowledge of the duty to preserve evidence after receiving the December 10, 2008 letter from plaintiffs' counsel. There is no evidence that he took any action to intercept the automatic deletion of relevant evidence. As such, recklessness and bad faith are permissible inferences.").

[32] For example, in *United States v. Philip Morris USA Inc.*, the Court granted in part and denied in part the United States' motion for sanctions against Philip Morris for spoliation of evidence, finding that eleven Philip Morris executives and officers "at the highest corporate level" violated the Court's document preservation order and Philip Morris's policies. 327 F. Supp. 2d 21, 25 (D.D.C. 2004).

[33] *See, e.g.*, 17 C.F.R. § 240.17a-4 (2018)—Records to be preserved by certain exchange members, brokers, and dealers (depending on the type of record, for either three or six years); 17 C.F.R. §§ 270.31a-1-a-3 (2018)—Records to be maintained by registered investment companies and certain other related persons; records to be preserved (some permanently, some for a period of years); 18 U.S.C. § 1519 (2018)—Destruction, alteration, or falsification of records in Federal investigations and bankruptcy (the so-called "anti-shredding provision").

Data analysis

A company might consider collecting relevant data for further review and analysis, such as, for example, trade data where trading misconduct is suspected. Such analysis may uncover trends in behavior, or point to particular dates or target areas of potential misconduct.

Interviews

If a company can identify individuals who may have knowledge regarding the conduct at the focus of a potential crisis, it may conduct preliminary informational interviews. Such informational interviews may provide early insight into the potential conduct at issue and shed light with respect to further documents and data that should be collected and reviewed. As discussed above, a company should also consider whether interviewees will be afforded individual counsel and if not, provide any necessary disclaimers.[34]

Maintaining a record

Throughout the investigation, it is important to create and maintain a record of all actions taken, which may be referenced in communications with any investigating authorities if questions arise later in the process. Such record may also assist in keeping the relevant stakeholders in the loop, both to avoid second-guessing and to ensure efforts are coordinated as the investigation unfolds. A company should also seek to determine whether any other investigations involving the company are underway, which may require coordination.

[34] For example, the company may choose to waive the privilege covering communications with company counsel, which would not protect the individual employees. *See Upjohn Co. v. United States*, 449 U.S. 383 (1981).

Maintaining Flexibility Throughout the Investigation

While the considerations discussed in this chapter will assist in ensuring that a company is prepared to address a potential crisis head-on through an effective first response, it is important to remember that it is virtually impossible to predict how an investigation will unfold and that no two situations or investigations are alike. For this reason, it is essential to maintain flexibility and be prepared to adapt a response plan as needed to effectively address any unforeseeable issues that may arise. Throughout this Handbook, we provide examples of how other companies have dealt with crises. Such examples are intended to be illustrative and provocative, but they are not prescriptive: just because one company has followed a particular playbook successfully in the past that does not mean that playbook will be the appropriate or required one in the event of your crisis.

Preparation Is Key

Finally, one of the best ways to prevent, or at the very least manage, a crisis is by maintaining an effective compliance program to detect and prevent misconduct, as well as an incident response plan, which are periodically assessed and updated. In particular, having an established incident response plan can help to ensure that the company is poised to respond quickly and effectively at the outset in the event that a crisis occurs. By carefully outlining the initial steps that a company should take, and appointing specific individuals to guide the response forward, such programs ensure that appropriate measures are in place in advance of a crisis. Further, it is equally important to train and prepare individuals within the company to employ these measures if needed. For example, tabletop exercises provide company personnel with opportunities to practice and improve how they will respond in the event that an actual crisis occurs. Moreover, in a constantly changing environment, it is critical that these plans are periodically tested and updated to remain relevant and effective.

Chapter II:
Responding to Requests From Authorities

Summary

Types of Requests

Compulsory Requests: Certain governmental requests are mandatory and enforceable by the relevant government agencies or a court. Such compulsory requests come in a variety of forms, including:

— Grand jury subpoenas;

— Administrative subpoenas;

— Search warrants;

— Financial industry regulatory requests; and

— State-level subpoenas.

Requests for Voluntary Disclosure: Other requests are non-compulsory and the receiving party is not legally required to comply, but may nonetheless determine that it is in its best interest to do so. If not satisfied, such requests sometimes are followed by compulsory requests.

Early Considerations

Upon receiving a compulsory or voluntary request, and throughout the investigation that follows, a company should consider certain issues, including:

— The nature and purpose of the investigation;

— Whether to seek to quash or modify a subpoena, or negotiate the scope of a request;

— Document retention;

— Legal limitations on data dissemination;

— The potential impact of decisions regarding production in response to one request on the company's ability to produce or withhold from production in response to requests from other jurisdictions; and

— Providing a timely and effective response in a way to minimize the chance for follow-on requests.

Introduction

In some instances, early strategic decisions concerning how to respond to a request for information can effectively work to limit, or at a minimum, frame the scope of additional inquiry. However, responses need to be carefully crafted to ensure that requesting authorities do not get the misimpression that a recipient is wary of fully complying or is hiding something. In addition, the sheer number of regulatory and criminal agencies, their varying powers to compel production, and their own internal practices and cultures further complicate what are generally the twin goals of responding to a request: (i) to get the requesting authority what it needs as efficiently as possible while maintaining credibility, and (ii) to appropriately cabin the scope of inquiry to the relevant subject matter to minimize the burden. In addition, there are important practical considerations that are best reviewed at the outset of receiving a request for information and kept in mind while responding, in order to protect privileged and other confidential information and to help ensure that the investigation progresses smoothly. This chapter discusses some of the different types of compulsory and voluntary requests a company may receive, discussing practices of specific agencies as examples only, as well as potential issues and strategies that should be considered in order to respond effectively.

Compulsory Requests for Information[1]

Grand Jury Subpoenas

In the United States, the grand jury's purpose is to determine whether charges against a suspect are warranted. The grand jury does not sit to determine guilt or innocence, but rather, to assess whether there is a basis to bring a criminal charge.[2] Accordingly, grand jury subpoenas are a compulsory process used by criminal prosecutors to pursue an investigation, through which the grand jury determines whether there is probable cause to believe a crime has been committed. As such, the grand jury is not required to make a preliminary showing of probable cause

[1] It is important to keep in mind, however, that there are many more criminal and regulatory authorities, both in the United States and elsewhere, and companies should consider the particular practices of each relevant authority on a case-by-case basis.

[2] *See* U.S. Const. amend. V ("No person shall be held to answer for a capital, or otherwise infamous [federal] crime, unless on a presentment or indictment of a Grand Jury").

before initiating an investigation, and a grand jury subpoena can be issued based on mere suspicion that the law is being violated or to seek assurance that it is not.[3]

Grand jury subpoenas have a substantially broader reach than subpoenas used in criminal or civil litigation, where the specific offense or conduct at issue has already been identified. In the absence of a probable cause requirement, the grand jury is empowered to issue broad requests for witness testimony (through a *subpoena ad testificandum*), as well as for documents, papers, and other physical evidence (through a *subpoena duces tecum*), which may include confidential information.[4] Notably, grand jury proceedings are conducted in virtually complete secrecy pursuant to the Federal Rules of Criminal Procedure and comparable state laws.[5]

Failure to comply with a grand jury subpoena may constitute civil or even criminal contempt.[6] Nevertheless, the grand jury's authority is not self-executing and it must rely on the courts to enforce a contempt order.[7] A party subject to a grand jury subpoena may seek to limit the subpoena's reach by moving to quash or modify the subpoena before a court; however, the court's ability to quash a grand jury subpoena is limited by a high standard of reasonableness, and the burden frequently is on the moving party to demonstrate that the request is unreasonable.[8] Courts may also quash or modify a grand jury subpoena on grounds that the materials or testimony sought are protected by a valid, recognized privilege, that the subpoena will infringe upon a constitutional right, or that the government has abused the grand jury process.[9] Abuse of the grand jury process occurs, for example, where a subpoena is used improperly to obtain information for a parallel civil litigation.[10]

---

[3] *United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991) (defining a grand jury as "an investigatory body charged with the responsibility of determining whether or not a crime has been committed").

[4] Fed. R. Crim. P. 17(c).

[5] Fed. R. Crim. P. 6(e)(2)(B).

[6] Fed. R. Crim. P. 17(g).

[7] *Id*. *See also United States v. Williams*, 504 U.S. 36, 48 (1992) ("[T]he grand jury cannot compel the appearance of witnesses and the production of evidence, and must appeal to the court when such compulsion is required.").

[8] *See R. Enters., Inc.*, 498 U.S. at 301("[A] grand jury subpoena issued through normal channels is presumed to be reasonable, and the burden of showing unreasonableness must be on the recipient who seeks to avoid compliance.").

[9] *See, e.g., Williams*, 504 U.S. at 48 ("[T]he court will refuse to lend its assistance when the compulsion the grand jury seeks would override rights accorded by the Constitution . . . or even testimonial privileges recognized by the common law.").

[10] *See, e.g., United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958) ("[The] 'indispensable secrecy of grand jury proceedings,' must not be broken except where there is a compelling necessity.")(citation omitted).

Administrative Subpoenas[11]

Subpoenas served by administrative agencies—for example, the U.S. Securities and Exchange Commission ("SEC" or "Commission"), the Office of Foreign Asset Control ("OFAC"), or the Department of Labor ("DOL"), among others—may serve a variety of purposes, including gathering information to issue future rules or regulations,[12] or to investigate and formally adjudicate suspected misconduct. Administrative subpoena power is derived from agency enabling statutes and regulations and can impart broad investigative authority on the relevant agency. Like grand jury subpoenas, administrative subpoenas generally do not require a showing of probable cause prior to issuance, and can be issued based "merely on suspicion that the law is being violated, or even just because [the agency] wants assurance that it is not."[13] Thus, administrative subpoenas often serve as powerful tools that enable U.S. government agencies to undertake broad investigations.

Notwithstanding the broad reach of administrative subpoenas, some caveats limit their power. For example, administrative subpoenas are subject to constitutional and jurisdictional limitations. Although the Supreme Court has sanctioned the broad investigatory powers of administrative agencies,[14] administrative subpoenas are still subject to the reasonableness standards of the Fourth Amendment, and will be found to comply "so long as it is 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'"[15] Likewise, agency enabling statutes apply jurisdictional limitations on the scope of an agency investigation.[16]

---

[11] Due to the wide variety of regulatory agencies, this chapter contains a general discussion of administrative subpoenas and some generally applicable considerations.

[12] *See, e.g., F.T.C. v. Brigadier Indus. Corp.*, 613 F.2d 1110 (D.C. Cir. 1979) (discussing the Federal Trade Commission's authority to issue subpoenas as part of its rule-making process).

[13] *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950); *see also United States v. Powell*, 379 U.S. 48, 51-53 (1964) (discussing absence of a probable cause requirement).

[14] *See, e.g., Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209, 214 (1946) (acknowledging the broad investigatory powers Congress may delegate to administrative agencies and that such "authority would seem clearly to be comprehended in the 'necessary and proper clause'").

[15] *Carpenter v. United States*, 585 U.S. ____, (2018) (Kennedy, J. dissenting) (quoting *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984)); *see also C. A. B. v. United Airlines, Inc.*, 542 F.2d 394, 395 (7th Cir. 1976) (refusing to enforce a subpoena when the administrative agency would not specify its investigative purpose or make its demand reasonably definite).

[16] *See United States v. Holstrom*, 242 F. App'x 397, 398 (9th Cir. 2007) (dismissing an indictment when the agency's enabling statute did not provide authority for such investigatory powers over the rail service).

Further, even where an agency has legal authority to issue a subpoena, agency staff may be required to obtain written authorization from senior officers within the agency before they can issue subpoenas, which can be a somewhat time-consuming process.[17] In addition, administrative subpoenas are not self-enforcing. Failure to comply with an administrative subpoena, standing alone, typically does not constitute contempt or expose the recipient to sanctions absent a court order. If a subpoenaed party fails to comply with a federal agency's request, the agency must petition the relevant federal district court to compel compliance.[18] The district court's ruling either for or against enforcement of the subpoena constitutes a final, appealable decision, and a subpoena recipient who violated that court order could be subject to a civil, or even criminal, contempt charge.[19]

When an agency seeks judicial enforcement of an administrative subpoena, courts will consider whether the agency can show "that the investigation will be conducted pursuant to a legitimate purpose, that the inquiry may be relevant to the purpose, that the information sought is not already within the [agency's] possession, and that the administrative steps required . . . have been followed."[20] Courts may refuse to enforce an agency subpoena, for example, where it can be shown that the subpoena was intended to harass or is unduly burdensome to the recipient.[21] At the time of judicial enforcement, the recipient can challenge the administrative subpoena, and bears the burden of demonstrating that it is invalid. This is a high bar, however, as courts typically do not permit discovery into agency motives for instituting an investigation unless the recipient is able to demonstrate facts indicating abuse.[22]

Thus, the non-self-enforcing nature of administrative subpoenas presents strategic considerations regarding the extent to which a company may choose to comply

[17] For example, SEC staff must receive a formal order of investigation—authorized by either the Commission itself or the Director of the Division of Enforcement—to issue subpoenas compelling testimony and the production of documents. The order describes the general nature of the investigation and identifies provisions of the federal securities laws that may have been violated. *See* 15 U.S.C. § 78u(a)-(b) (2018); *How Investigations Work*, Sec. Exch. Comm'n, https://www.sec.gov/enforce/how-investigations-work.html (last visited July 25, 2018).

[18] *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 741 (1984) ("Subpoenas issued by the Commission are not self-enforcing, and the recipients thereof are not subject to penalty for refusal to obey. But the Commission is authorized to bring suit in federal court to compel compliance with its process.").

[19] *See* 5 U.S.C. § 555 (d) (2018).

[20] *Powell*, 379 U.S. at 57-58.

[21] *Id*. U.S. at 58 ("Such an abuse would take place if the summons had been issued for an improper purpose, such as to harass . . . or to put pressure . . . to settle a collateral dispute, or for any other purpose reflecting on the good faith of the particular investigation.").

[22] *See, e.g., id.*; *United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 316-17 (1978); *United States v. Judicial Watch, Inc.*, 241 F. Supp. 2d 15, 17 (D.D.C. 2003).

at the outset. On one hand, there may be latitude for recipients to negotiate an administrative subpoena's scope, as agency staff may be willing to work with recipients rather than expending the agency's time and resources to seek judicial enforcement. On the other hand, given the broad investigative authority and great deference afforded to federal agencies by courts, refusal to comply with an agency subpoena may only serve to delay the investigation and potentially antagonize the requesting agency.

State-Level Subpoenas

State-level administrative and civil subpoenas, which vary by state, are utilized by authorities at the state level to require the production of certain documents or information. In New York, for example, the Department of Financial Services ("DFS") has statutory authority to "subpoena witnesses, to compel their attendance, to administer an oath, to examine any person under oath and to require the production of relevant books or papers."[23] The New York Attorney General's Office ("NYAG"), which has general authority to conduct investigations into securities or commodities fraud and to bring civil and criminal actions, also has broad power to issue subpoenas statewide to compel the appearance of witnesses or the production of documents in connection with an investigation under the Martin Act.[24] Failure to comply with a DFS or NYAG subpoena constitutes a misdemeanor.[25]

Other Compulsory Requests

Civil Investigative Demands

An increasingly common form of compulsion is the Civil Investigative Demand ("CID"), which is used to obtain documentary information, answers to interrogatories, and oral testimony when there is reason to believe that a party has engaged in certain misconduct or wrongdoing. CIDs, which are authorized by statute, are typically quite broad in scope, and permit the federal government to investigate and determine whether there is sufficient evidence to justify the expense

[23] N.Y. Banking Law § 38 (2018).

[24] It is widely recognized that the powers granted to the New York Attorney General under the Martin Act are very broad. *See Anwar v. Fairfield Greenwich Ltd.*, 728 F. Supp. 2d 354, 367 (S.D.N.Y. 2010) (describing the Martin Act as "a statute of enormous breadth and unique dimensions.") (quoting *D'Addio v. L.F. Rothschild. Inc.*, 697 F. Supp. 698, 707 (S.D.N.Y.1988)); *see also* N.Y. Gen. Bus. Law § 352(2) (2018) (The Martin Act).

[25] N.Y. Gen. Bus. Law § 352(4) (2018); N.Y. Banking Law § 38 (2018).

of pursuing litigation. For example, the Department of Justice ("DOJ") may issue CIDs where the government is investigating antitrust violations, False Claims Act ("FCA") violations, or civil racketeering.[26] Financial industry regulators, such as the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB"), may also have authority to issue CIDs seeking documents, responses to interrogatories, tangible items, or deposition testimony.[27]

National Security Letters

National security letters ("NSLs") allow the Federal Bureau of Investigation ("FBI") to gather information for purposes of national security. Authorizing statutes specify the type of information that may be sought via NSL, including subscriber information and toll billing records, consumer identifying information, and financial records.[28] The FBI can issue NSLs without obtaining prior approval from a judge,[29] and recipients are often subject to gag orders and prohibited from sharing the fact that they have received an NSL.[30] To challenge an NSL, a recipient may "petition for an order modifying or setting aside the request" in the federal district court where the NSL recipient does business or resides, and the court may modify or set aside the request if it finds that compliance would be "unreasonable, oppressive, or otherwise unlawful."[31] Similarly, the Attorney General must go to the district court in the jurisdiction in which the investigation is taking place or the recipient resides, does business, or may be found, to compel compliance.[32]

[26] *See* 15 U.S.C. § 1312 (2018) (antitrust); 31 U.S.C. § 3733 (2018) (false claims); 18 U.S.C. § 1968 (2018) (racketeering).

[27] *See* 15 U.S.C. § 57b-1 (2018) (FTC); 12 U.S.C. § 5562 (2018) (CFPB).

[28] The FBI's authority to issue NSLs is derived from several statutes, including: the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2018) (government permitted to request subscriber information and toll billing records); the Fair Credit Reporting Act, 15 U.S.C. § 1681u (2018); the Right to Financial Privacy Act, 15 U.S.C. § 1681v (2018) (government permitted to request consumer identifying information); and 12 U.S.C. § 3414 (2018) (government permitted to request financial records).

[29] 12 U.S.C. § 3414(a)(5) (2018).

[30] *See, e.g.*, 18 U.S.C. § 2709(c)(1) (2018).

[31] 18 U.S.C. § 3511(a) (2018).

[32] 18 U.S.C. § 3511(c) (2018).

Search Warrants

In addition to grand jury and administrative subpoenas, criminal authorities may use search warrants as tools to seize physical and electronic evidence. Search warrants are written orders issued by a federal district or magistrate judge directing law enforcement agencies to search specific premises and to seize specific persons or property.[33] The warrant must specify the person or property to be searched or seized.[34] Unlike grand jury or administrative subpoenas, the district or magistrate judge must find probable cause that a crime has been committed before issuing a warrant.[35] In addition, unlike subpoenas, which typically afford recipients time to respond, search warrants authorize law enforcement and government agencies to immediately seize the evidence they are seeking. Whereas a subpoena can be quashed in certain circumstances or must otherwise be enforced, a company often has no legal recourse to prevent the execution of a search warrant and, in most cases, a challenge can only be made after the fact,[36] typically in the form of a pre-trial motion to suppress and/or a motion for return of property.[37]

Financial Industry Regulatory Requests

Outside of subpoenas and warrants, there are a number of financial industry regulatory or self-regulatory agencies that have authority to issue compulsory

[33] Fed. R. Crim. P. 41(b).

[34] Fed. R. Crim. P. 41(e)(2)(A).

[35] Fed. R. Crim. P. 41(d)(1).

[36] *See Dalia v. United States*, 441 U.S. 238, 239 (1979) ("[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness."). It is worth noting that there may be limited occasions where companies can resist and successfully challenge government warrants in certain contexts. For example, the Stored Communications Act ("SCA"), which provides that the government can issue a warrant for service providers to provide certain customer information, contains a mechanism by which service providers can challenge or move to quash such warrants. 18 U.S.C. § 2703(d) (2018). The ability of the United States government to compel data stored abroad pursuant to the SCA was recently clarified through the introduction of the Clarifying Lawful Overseas Use of Data ("CLOUD") Act, which provides a mechanism for service providers to challenge or move to quash warrants issued pursuant to SCA, seeking disclosure of electronic communications stored exclusively on servers at datacenters abroad. *See* CLOUD Act § 103(a)(1), codified at 18 U.S.C. § 2713 (2018). By introducing a procedure for pre-enforcement challenges to SCA warrants, the CLOUD Act effectively aligns such warrants with the procedures for enforcing subpoenas, discussed above.

[37] Under Federal Rule of Criminal Procedure 41(g), a "person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). Rule 41(h) likewise allows a defendant to move to suppress evidence. In a recent and highly publicized example, in April 2018, the FBI executed broad search warrants for President Trump's former lawyer and associate Michael Cohen's residence, hotel room, office, safety deposit box, and electronic devices. Although Mr. Cohen could not prevent the execution of the warrant, his counsel immediately requested that the seized materials be returned to Mr. Cohen's counsel for initial review and production, and then moved for a temporary restraining order to prevent the government from reviewing the materials. In the Southern District of New York, the Court ultimately resolved the issue by appointing a special master to review the documents for privilege. *See* Order of Appointment, *Michael Cohen v. United States*, No. 18-mj-03161 (S.D.N.Y. Apr. 27, 2018), ECF No. 30.

requests to entities that fall within their regulatory ambit.[38] Self-regulatory organizations ("SROs"), for example, supplement the SEC's regulatory authority.[39] The SEC delegates to SROs the ability to regulate their members, including authority to discipline, expel, and suspend members for conduct "inconsistent with just and equitable principles of trade."[40] One of the more notable SROs is FINRA, which regulates the broker-dealer community, and has authority to investigate conduct that violates the securities rules through discovery requests for documents and information, as well as authority to fine, suspend, or bar broker-dealers who do not comply.[41] There are a host of other SROs in addition to FINRA, including, for example, the New York Stock Exchange ("NYSE"), which have authority similar to FINRA's over their members.[42] The SEC has supervisory authority over FINRA and other SROs, and may abrogate or change their rules.[43] To challenge a FINRA request, the recipient must refuse compliance and appeal any disciplinary action to the SEC.[44]

It should be noted that SROs' power over their members is generally very broad. For example, FINRA and the NYSE have taken the position that merely refusing to produce documents in response to a request or appear for testimony constitute violations of their rules that can, standing alone, result in disciplinary proceedings, resulting in fines, bars, or other sanctions, irrespective of whether a substantive violation of the securities laws can be shown.

---

[38] Relevant financial industry regulatory agencies include the SEC, the Financial Industry Regulatory Authority ("FINRA"), the Federal Reserve Bank (the "Fed"), the Commodity Futures Trading Commission ("CFTC"), the FTC, the CFPB, and the Office of the Comptroller of the Currency ("OCC"), among others.

[39] SROs are non-governmental organizations authorized by Congress to create and enforce industry regulations and standards. *See* Section 10B(c) of the Securities Exchange Act of 1934.

[40] 15 U.S.C. § 78f (2018).

[41] FINRA Rule 8210 grants FINRA authority to inspect and copy books, records, and accounts of member firms. *See Information and Testimony Requests*, Fin. Industry Reg. Auth., http://www.finra.org/industry/information-and-testimony-requests (last visited Aug. 1, 2018); *What We Do*, Fin. Industry Reg. Auth., https://www.finra.org/about/what-we-do (last visited Aug. 1, 2018).

[42] NYSE Regulation ("NYSER") is responsible for monitoring activities on the NYSE's exchanges, and for addressing non-compliance by NYSE members with the NYSE's rule and the applicable federal securities laws. While some regulatory functions are performed directly by NYSER, others are performed by FINRA or another self-regulatory organizations pursuant to a regulatory service agreement. Disciplinary Actions stem from a variety of sources, such as internal referrals, investor complaints, examinations of member organizations, and referrals from the SEC. *See NYSE Regulation*, New York Stock Exch., https://www.nyse.com/regulation (last visited July 25, 2018).

[43] *See* 15 U.S.C. § 78s(b)(7)(C) (2018).

[44] *See In re Application of Jay Alan Ochanpaugh*, No. 3-12147, 2006 SEC LEXIS 1926, at *21 (Sec. Exch. Comm'n Aug. 25, 2006).

PRACTICE TIP: CONSIDERATIONS OF INTERNATIONAL FINANCIAL INSTITUTIONS AND DEVELOPMENT ORGANIZATIONS

In addition to requests from U.S. government regulators, international financial institutions and development organizations, such as the World Bank Group (the "World Bank"), may also make requests or solicit information, particularly through contractual audit rights.[45] Although the World Bank does not have formal subpoena power, failure to comply with a request may nevertheless constitute a sanctionable offense with broad commercial consequences.[46]

— The World Bank can issue a Notice of Temporary Suspension, temporarily suspending a respondent from entering into new contracts with the World Bank,[47] but it can also initiate more formal proceedings with a wide range of possible sanctions:

- **Reprimand:** The sanctioned party is formally reprimanded;[48]
- **Conditional Non-Debarment:** The sanctioned party is required to comply with certain remedial, preventative, or other conditions in order to avoid debarment from World Bank Projects;[49]
- **Debarment:** The sanctioned party is declared ineligible (either indefinitely or for a specified period of time) from benefiting from participation in certain Bank-financed contracts or projects.[50]
- **Debarment with Conditional Release:** The sanctioned party is only released from debarment if it demonstrates compliance with certain remedial, preventative, or other conditions for release, after a specified period of debarment.[51]
- **Restitution:** The sanctioned party must pay restitution to remedy the harm caused by its misconduct.[52]

[45] World Bank Grp., *The World Bank Group's Sanctions Regime: Information Note12* (Nov. 2011), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/The_World_Bank_Group_Sanctions_Regime.pdf..

[46] World Bank Grp., *World Bank Group Sanctions Procedures*, Appendix 1 (Apr. 2012), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/WBGSanctions_Procedures_April2012_Final.pdf.

[47] *Id*. at Article II, § 2.01.

[48] *Id*. at Article IX § 9.01(a).

[49] *Id*. at Article IX § 9.01(b).

[50] *Id*. at Article IX § 9.01(c).

[51] *Id*. at Article IX § 9.01(d).

[52] *Id*. at Article IX § 9.01(e).

— Debarment can be particularly burdensome to companies as it extends to other development banks that have entered into a "cross-debarment agreement" with the World Bank cross acknowledging debarments by other multilateral banks.[53]

— One point to consider is the impact that disclosure to institutions such as the World Bank could have on privilege protections. While privileged materials are considered exempt from disclosure in World Bank sanctions proceedings,[54] if such materials are disclosed it could constitute a privilege waiver.[55]

Responding to Compulsory Requests

PRACTICE TIP:
CHALLENGING OR NEGOTIATING AN ADMINISTRATIVE SUBPOENA—QUESTIONS TO CONSIDER

— Does the requesting agency have jurisdiction?

— Does the scope of the subpoena go beyond the reasonable needs of the investigation?

— Was the subpoena issued pursuant to a legitimate purpose of the agency, and does it comply with the authority granted through the agency's enabling statute?

— Is the request overly vague or indefinite?

— Was the request made in good faith or for an improper purpose?

— Does the subpoena violate a constitutional right or request privileged information?

[53] These include the Asian Development Bank, African Development Bank, European Bank for Reconstruction and Development, and the Inter-American Development Bank. *See* World Bank Grp., *The World Bank Group's Sanctions Regime: Information Note 9* (Nov. 2011), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/The_World_Bank_Group_Sanctions_Regime.pdf.

[54] World Bank Grp., *World Bank Group Sanctions Procedures*, Article VII § 7.02 (Apr. 2012), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/WBGSanctions_Procedures_April2012_Final.pdf.

[55] For more information on preserving legal privilege, *see* Chapter [IV]: [Preserving Legal Privilege].

Early Considerations When a Company Receives a Compulsory Request

Upon receipt of a compulsory request for information, counsel and the company should first consider whether the requesting authority has jurisdiction to issue such request, and whether lack of jurisdiction limits the company's obligation to respond. Jurisdictional considerations should be given appropriate weight *before* responding to a request, as an improvident exchange of information with an agency that does not have jurisdiction can result in a waiver of jurisdictional arguments.

Once jurisdiction and other legal authority is established, counsel and the company should consider initiating an early discussion with the issuing authority, to build rapport and better understand the underlying purpose of the request. In addition, counsel and the company should consider whether to request an extension of time to respond, and whether the information requested can be narrowed through negotiations with agency staff. Where counsel has established credibility and demonstrated a willingness to cooperate, authorities may be open to engaging in some discussion in an effort to accelerate their access to relevant information and ultimately expedite their investigation. In addition, in industry-wide investigations, it may be useful to engage in joint-defense discussions with peer institutions who may be further along in the investigation process, to gain additional information before preparing a response.

PRACTICE TIP: EARLY CONSIDERATIONS UPON RECEIPT OF A REQUEST FOR INFORMATION

— **Scope.** Consider whether to discuss the subject matter of the request with the issuing authority to better understand its purpose and explore whether it would be possible to narrow its scope.

— **Timing.** Consider whether the schedule in place for the production of documents and information is reasonable, and whether a request for an extension of time is warranted. In cases where a large volume of information is requested, consider proposing a schedule for partial productions to be made at regular intervals. Because credibility is an important factor, it is usually better to set reasonable and realistic expectations at the outset, rather than running up against deadlines and needing to seek additional time after the fact.

— **Purpose.** Consider the purpose of the investigation and the company's role to determine how best to respond to the request. In particular, it may be helpful to clarify with the issuing authority whether the relevant government agency considers the company a witness, subject, or target.[56]

— **Quash or modify.** Consider whether there may be grounds to quash or modify the subpoena or request, or opportunities to negotiate its scope, as well as whether there are any legal limitations on the data that can be provided in response.

— **Custodians.** Immediately upon receipt of a request for document production, consider which custodians are likely to have relevant information. This is not only necessary to collect and retain relevant documents, but will allow a company to get a leg up on both understanding the scope and subject matter of the request and possibly negotiate for a narrower production.

— **Document retention and custodian of records.** Promptly prepare a litigation hold notice to circulate to employees, as well as a certification for employees to acknowledge compliance, and consider suspending regular document deletion or destruction procedures. It may also be helpful to appoint a custodian of records at the company to liaise with counsel to ensure compliance with the request. Also

[56] The terms "subject" and "target" are commonly used in the criminal context to characterize the role of a company or individual being investigated in contrast to a witness, which is primarily viewed as a source of information rather than a focus of the investigation. The U.S. Attorney's Office Manual defines a "subject" of an investigation as "a person whose conduct is within the scope of the grand jury's investigation," and a "target" as "a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant." Dep't of Just., *U.S. Attorneys' Manual* § 9-11.151 (Nov. 1997) ("USAM"). Some civil agencies—particularly those that often investigate potential misconduct in conjunction with criminal authorities—are also familiar with, and use, this lexicon. While some agencies may not use the same designations, they may nonetheless be willing to discuss the nature of the investigation. The SEC, for example, does not identify "targets" of its investigations; it does, however, issue formal investigation orders which describe the nature of the investigation, and can be requested by a party subject to investigation. *See* Sec. Exch. Comm'n, *Enforcement Manual* §§ 3.3.2, 2.3.4.2 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

consider alerting the company's human resources or information technology department that normal document retention procedures should be suspended and documents should be retained until further notice for departing employees who may have relevant documents.

— **Joint defense.** Consider whether entering into any joint defense agreements—for example, with individual counsel for represented employees or with peer institutions subject to the same investigation—would be useful.

Limitations on Data Dissemination

In the early stages of responding to a compulsory request, companies should consider whether any legal protections might limit their obligation, and indeed their legal ability, to produce the requested information, to avoid inadvertently including such information in a response. Some protections that should be considered at the outset include:

Jurisdictional Limitations

As discussed above, a company should first consider whether there are jurisdictional limitations to the requesting authority's legal ability to issue the request and/or collect certain documents and information. This is often a fact-intensive inquiry, which turns on factors such as the requesting authority's location and jurisdictional authority, the location of the company and its affiliates, and the location of the documents and individuals to be produced.[57] For example, it is not unusual for subpoenas to be served on corporate entities present in the United States, to reach an entity located in another jurisdiction which "owns" the documents sought by the subpoena. Such entity may be a parent company, a subsidiary, or an affiliate with no U.S. presence. Responsibility to produce requested information can turn on whether the domestic affiliate has sufficient control of the responsive overseas documents to render them subject to production in the United States.[58]

[57] It should be expected that agencies will argue that deference should be given to their interpretations of their own jurisdictional limitations, particularly at the investigatory stage. *See F.T.C. v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) ("as a general proposition, agencies should remain free to determine, in the first instance, the scope of their own jurisdiction when issuing investigative subpoenas") (citing *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501 (1943)).

[58] *See In re Canadian Int'l Paper Co.*, 72 F. Supp. 1013, 1020 (S.D.N.Y. 1947) (In grand jury proceedings: "The test [for the production of documents] is control— not location").

Attorney-Client Privilege and Attorney Work-Product

In the United States, attorney-client privilege protects against disclosure of communications between a lawyer and client made for the purpose of seeking or providing legal advice, and extends to communications made during the course of an internal investigation between a company's employees and the company's counsel.[59] The work-product doctrine protects against disclosure of documents (or other tangible items) containing mental impressions, opinions, or legal theories prepared in anticipation of litigation.

The rules regarding privilege and work product differ depending on the jurisdiction whose laws apply, and it will be important to be sensitive to the choice-of-law issues as well as the substantive law of privilege in the relevant jurisdictions. As discussed above, materials covered by either attorney-client privilege or attorney work-product need not be disclosed in response to a compulsory request. However, consideration of these protections at the outset is critical, as they may be inadvertently waived.[60]

Confidential Supervisory Information

Financial institutions supervised by the Board of Governors of the Federal Reserve Bank (the "Board") may have access to confidential supervisory information ("CSI"), which is subject to the Board's regulations governing its disclosure.[61] In practice, CSI covers information related to the examination of a financial institution by a bank examiner.[62] Because all CSI remains the property of the Board, no supervised institution or individual, to whom the information has been made available, may disclose such information without the prior written consent of the Board's general counsel, unless a specified exception applies.[63]

Suspicious Activity Reports

Banks are required to file suspicious activity reports ("SARs") with the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), upon detecting

---

[59] *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).

[60] For a more detailed discussion of legal privilege, *see* Chapter IV: Preserving Legal Privilege.

[61] *See generally* 12 C.F.R. § 261 (2018).

[62] *See* 12 C.F.R. § 261.2(c)(1)(ii)-(iii) (2018). Relevant bank examiners include the Fed, the OCC, DFS, the CFPB, and the Federal Deposit Insurance Corporation ("FDIC"), among others.

[63] *See* 12 C.F.R. § 261.20(g) (2018). Upon request, the Board may make CSI available to federal or state financial institution supervisory agencies, and may authorize other discretionary disclosures of CSI as necessary. *Id.* at § 261.20 (c), (d), (e) (2018).

or suspecting that a crime is taking place.[64] Banks may be required to submit SARs in certain circumstances, or may report suspicious activities voluntarily. In either case, SARs are confidential and may not be disclosed except as specified by statute and in FinCEN's regulations; statutory and regulatory exceptions may allow disclosure of SARs to certain law enforcement and supervisory agencies.[65]

Blocking Statutes or Restrictions on Cross-border Data Transfers

Blocking statutes are enacted by certain jurisdictions to prohibit exporting documents for use in judicial or administrative proceedings without government consent.[66] Data privacy laws similarly restrict cross-border access to information stored in certain countries, particularly in the EU.[67] Even where there is no applicable blocking statute or data privacy law, certain foreign authorities may require that they be notified of a request that implicates data or documents stored in their jurisdiction, and may further require that the information be provided through the local authority as a conduit. For example, the UK Financial Conduct Authority ("FCA") sets forth procedures by which information stored in the UK must be produced pursuant to a Notice of Requirement ("NOR").[68]

It is important to consider the importance of blocking statutes or similar other restrictions at the very beginning of an inquiry before any documents are collected. Decisions with respect to where to view documents and whether to transfer documents from a jurisdiction that has a blocking statute to one that happens not to have such a statute can have dramatic—and sometimes unintended—consequences for a later stage of the investigation when the documents are requested. Companies should, therefore, be mindful of not running afoul of laws restricting cross-border transfers of documents and information, particularly where a company has offices in other jurisdictions. Moreover, such jurisdictional requirements may provide an opportunity to negotiate narrowing the scope of a request, in the interest of obtaining

---

[64] Fin. Crimes Enforcement Network, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions* 80 (2012), https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf.

[65] *See, e.g.*, 31 U.S.C. § 5318(g) (2018); 31 C.F.R. § 103.18(e) (2018); 12.C.F.R. § 21.11(k) (2018).

[66] 3 Robert L. Haig, *Business and Commercial Litigation in Federal Courts* § 21:97 (4th ed. 2017).

[67] *See* Council Directive 95/46, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31; General Data Protection Regulation (GDPR) 2016/679, 2016 O.J. (L. 119) 1. Data privacy and blocking statutes, including the European Union's recently enacted GDPR, are discussed in further detail in Chapter V: Data Privacy & Blocking Statutes.

[68] *See* Financial Services and Markets Act 2000 §§ 169 (Investigations in support of overseas regulator), 195 (Exercise of power in support of overseas regulator) (Eng.).

approval from the foreign authority to facilitate the production of the information sought by the requesting authority.

Other Confidential Information

In some instances, information that may not be covered by a statutory or other legal doctrine may still be protected from disclosure. For example, in the case of personally identifiable information ("PII"), which can be used to identify an individual in context (for example, name, social security number, passport number, driver's license number, address, or phone number), authorities may be amenable to redaction where the PII would be irrelevant to the purpose of their investigation. In addition, where PII is produced, there may be statutory limitations on further disclosure by the relevant authority,[69] or the authorities themselves might offer procedures by which a company can seek confidential treatment.[70]

Companies may also have entered into confidentiality agreements with clients or customers restricting their ability to disclose certain information. Although standard non-disclosure agreements typically include contractual provisions accounting for the possibility of compulsory requests, they also frequently have notice provisions that must be carefully considered and analyzed before documents are produced. In addition, there may be common law provisions that provide exceptions to confidentiality for government requests. Companies might also consider requesting confidential treatment following the production of such information, to limit further disclosure and any collateral liability under the terms of an applicable contract.[71]

[69] *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2018) (governing disclosure of PII). It should be noted, however, that prohibitions against disclosure may not apply where such disclosure is required by the Freedom of Information Act, or where another federal, state, or local government requests such information for purposes of civil or criminal law enforcement. 5 U.S.C. § 552a(b)(2), (b)(7) (2018).

[70] *See e.g.*, 17 C.F.R. § 200.83 (2018) (setting forth a procedure by which those submitting information to the SEC may request that it not be disclosed pursuant to a request under the Freedom of Information Act).

[71] For example, the SEC Enforcement Division may enter into confidentiality agreements with a company subject to investigation, by which the SEC would agree not to assert privilege waiver as to a third party of documents produced by the company that it would otherwise withhold as privileged. *See* Sec. Exch. Comm'n, *Enforcement Manual* § 4.3.1 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. In addition, the SEC might agree to maintain confidentiality over certain materials provided by a company, "except to the extent that the staff determines that disclosure is required by law or that disclosure would be in furtherance of the SEC's discharge of its duties and responsibilities." *Id*.

Negotiating the Scope of the Request

In addition to working through the practical considerations of responding to a request—identifying the relevant custodians, collecting and retaining relevant documents, and determining whether the request is within the agency's authority—consideration should also be given to negotiating the scope of the request.

Quite often agency requests are broadly drawn. There are numerous reasons for this, including that agency attorneys are often at the beginning of an investigation and wary of missing relevant information. Careful consideration should be given to whether to attempt to negotiate the precise scope of a request at the outset. A discussion about how a request can be narrowed may help the government by assisting it in targeting the documents that will be most relevant to its investigation and imposing on the company (rather than the government) the obligation to separate the "wheat from the chaff." At the same time, a discussion regarding narrowing a request may buy the company needed goodwill from the government, may reduce the costs of document production, and might avert the production of documents that while irrelevant lead to a broadening of the government investigation. Agencies are often amenable to such negotiations because—assuming that responding counsel has credibility and rapport with the agency—they can lever the company's expertise to help focus them on the documents most relevant to their inquiry. Moreover, the company and its counsel typically better understand the industry and are thus often better equipped to provide the most relevant information in the shortest possible time. Finally, from the agency's perspective, there is likewise value in building rapport and trust—it often means that companies will work to provide information beyond the strict limits of the request or, indeed, the agency's subpoena power, for example, by preparing reports, presentations, or interrogatory responses that are both, strictly speaking, beyond many agencies' subpoena power and highly useful in focusing on the most critical evidence. Government attorneys, who often face their own resource limitations, would also like to avoid the proverbial "document dump."

In negotiating the scope of a response, there are a number of considerations to keep in mind:

— ***Establish a dialogue.*** Initiating an early conversation may help to establish an ongoing dialogue with the investigating authority. Establishing an ongoing dialogue at the outset of the investigation helps to set the stage for negotiating the scope of the request, while keeping the door open for further negotiations down the road. Initiating a dialogue also demonstrates to the requesting authority that the company is taking its request seriously and is endeavoring to respond appropriately.

— ***Try to determine what is motivating the request.*** Keeping an open dialogue will not only build trust, but may help in determining which of the requests is most important to the relevant agency. In turn, this can help the company propose ways to narrow the focus of the request in a way that alleviates the burden on the company while getting the government what it is most interested in as quickly as possible.

— ***Propose an investigative strategy.*** Propose search terms and custodians for a document review, and consider offering to conduct a limited internal investigation short of a full-blown review to determine whether there may be additional ways to reduce the scope of the initial request. In seeking to narrow a request, it is critical to ensure the government understands that the company is not simply seeking to avoid unnecessary burden, but also to increase the efficiency of the investigation.

— ***Propose a schedule, including rolling productions.*** If the information requested will take considerable time to review and prepare for production, for example, due to the volume requested or data restrictions in other jurisdictions, consider proposing a schedule for providing partial responses on a regular basis through rolling productions. To the extent possible, such productions should be organized in a logical manner (e.g., by date, topic, or custodian), and with input from the requesting authority.

— ***Schedule regular check-in calls.*** After an initial conversation is had, regular "check-in" calls to discuss productions and the progress of the investigation serve to keep lines of communication open, apprising the requesting authority of progress while simultaneously helping the company proactively gauge whether the requesting authority is satisfied with the company's response to date. This helps the company steer its investigation in real time, rather than receiving after-the-fact notification that productions have been off-base or insufficient.

— ***Always do what you say you will.*** As discussed, credibility and rapport are critical to maintaining a smooth investigative process. As such, it is almost always better to be upfront about challenges and realistic about timeframes. While a company must avoid creating the impression that it is stonewalling an agency, overpromising and then needing to seek extensions or changes to the investigative plan is almost always worse than proposing reasonable deadlines, explaining why they are necessary, and sticking to them. Indeed, such frankness will often pay dividends both when it is necessary to revise a schedule and when negotiating a resolution at the end of the road.

Requests for Voluntary Disclosure

Government authorities also often request voluntary production of information. The reasons the government may issue voluntary requests can vary, but may include that the relevant regulatory or law enforcement authority (i) has not reached the stage of an investigation where it has compulsory power to issue subpoenas; (ii) views the company as merely a fact witness (as opposed to the target or subject of an investigation) and determined that seeking voluntary disclosures reflects a less aggressive posture; or (iii) determined that the company is, in any event, likely to comply fully with a voluntary request given the desire to remain on good terms with regulators and other authorities. From the company's perspective, it is frequently beneficial to receive a voluntary request rather than a compulsory request. Such voluntary requests not only do not have the force of law, but also may not give rise to the same disclosure issues as compulsory requests.[72] Voluntary requests may be made in the form of a letter or orally. A number of factors inform whether and to what extent a company should comply with a voluntary request for information,

[72] For further discussion of disclosure obligations, *see* Chapter IX: Collateral Considerations.

including the likely benefits of voluntary cooperation, the drawbacks of providing the law enforcement or regulatory agency with information it may not otherwise be able to obtain, and the legal barriers to complying fully with a voluntary request.[73]

In general, a voluntary request may provide more leeway for the recipient to frame the inquiry, as authorities may be more amenable to negotiating the scope of a request in the case of voluntary disclosure. Additional reasons to respond to a voluntary request include the ability to proactively build a positive rapport with the investigating authority (especially one with which the company is likely to come into contact in the future in the event that the agency concludes there has been wrongdoing), and to receive credit for cooperation, which may potentially reduce penalties down the line. In addition, the recipient of a voluntary request should not forget that the requesting authority likely has the power to issue a compulsory request if it deems an entity's voluntary response to be inadequate. Thus, a voluntary response may be viewed as an opportunity to avoid being subjected to a formal investigation. When presented with a voluntary request, therefore, the key objective is to strike a balance between providing a satisfactory response while maintaining the appropriate limitations on disclosure.

In responding to a request for voluntary disclosure, a company should similarly consider the points discussed above in the context of compulsory requests. However, where disclosure will be made voluntarily, the company may have greater latitude in framing its response, including whether to withhold information. This stands in contrast to a compulsory request, where the company risks being penalized if it withholds information absent a legal restriction on its ability to produce the information requested. Thus, in the context of a voluntary request, further consideration may be given to how best to respond while reducing the burden on the company, and making suggestions to the requesting agency to achieve this balance.

[73] Considerations relating to voluntary disclosures are discussed in further detail in the context of cooperation in Chapter VII: Cooperation.

PRACTICE TIP:
CONSIDERATIONS IN RESPONDING TO VOLUNTARY REQUESTS

Potential benefits:

— Ability to build a positive record and gain credibility.

— Potential to receive cooperation credit, which could lead to leniency.

— Increased latitude to frame the inquiry and potentially avoid a subsequent compulsory request.

Potential drawbacks:

— Potential to provide information to which a requesting authority may not otherwise have access.

— Lack of control over how authorities will utilize the information provided.

— Confidentiality concerns and disclosure restrictions.

— A company may be restricted from producing certain documents or information absent a compulsory request.

Conclusion

In sum, a company should give early consideration to the best method of providing the requested information as effectively and expeditiously as possible, regardless of whether the request is compulsory or voluntary. If the company has an obligation to respond or the investigating authority has jurisdiction, an overarching goal may be to provide a satisfactory response while advocating for the most favorable outcome to the company. Thus, giving due consideration at the outset to the various issues that may come into play will go a long way in strategizing how to frame an appropriate response and potentially negotiating the scope of the request. This will not only facilitate the progress of the investigation and garner credibility with the requesting authority, but will also help increase the likelihood of obtaining a favorable outcome.

Chapter III: Conducting an Internal Investigation

Summary

Investigation Lifecycle:

— Establish the Investigative Plan
  - Define scope
  - Determine goals
  - Identify key personnel
  - Create a timeline

— Initial Background Fact Gathering

— Document Collection/Review
  - Identify custodians
  - Collect potentially relevant documents
  - Implement a review protocol

— Conduct Interviews
  - Determine individuals who are likely to have knowledge of key events, evidence, or other relevant facts
  - Identify whether any employees need individual counsel
  - Review relevant materials in preparation for the interviews
  - Memorialize interviews

— Reporting and Disclosing Investigation Results
  - Identify the audience(s)
  - Determine the best format for reporting information

— Potential Responsive Actions
  - Improvements to corporate compliance policies and/or procedures
  - Potential disciplinary action against any employee(s) who committed misconduct
  - Consider whether to self-report to law enforcement authorities
  - Analyze market disclosure requirements and considerations

Introduction

Conducting an internal investigation while managing a global crisis can be a daunting task. An internal investigation is often necessitated by a crisis situation, so that a company can get to the bottom of what occurred, stop any ongoing conduct that could make matters worse, identify the appropriate remedial measures, be in a position to answer questions from auditors or other relevant internal or external constituencies, and anticipate and respond to any potentially related government investigations. When multiple jurisdictions are involved, expertise is required in understanding the impact of the various applicable laws on how the investigation should be conducted, including with respect to attorney-client privilege and data privacy rules.

Planning for and conducting internal investigations requires careful consideration and a well-developed strategy tailored to the company, the particular type of suspected or alleged misconduct, the interests of the company, and the likely regulatory and other external and internal expectations. For that reason, no two investigations will be conducted in exactly the same manner. However, there are certain generally applicable principles that are ordinarily considered and followed as best practices when conducting an internal investigation. This chapter sets out the most important components of the investigation lifecycle and describes the fundamental principles of conducting an effective internal investigation.

Establishing the Investigative Plan

An internal investigation should begin with the development of an investigative plan. While the form and length of such a plan can vary based on the circumstances, having an investigative plan is an important first step in any internal investigation to establish guidance and parameters for the investigators and other stakeholders who will be overseeing the investigation. The investigative plan will serve as the roadmap throughout the investigation and will often be a "living document" that will be modified once the investigation gets underway. The core components of any investigative plan include defining the investigation's scope, identifying the goals of the investigation, determining who will be overseeing and conducting the investigation, and setting an anticipated timeline for the investigation.

Define the scope

It is critical to determine the particular scope of an investigation at the outset to ensure the right issues are being investigated and resources are being used effectively, and then to periodically reassess that scope as time passes or in response to specific events. Determining the initial scope of an investigation is sometimes a straightforward exercise, but it can also be more nuanced, particularly when information about the conduct at issue is scant at the initial stages. Nevertheless, endeavoring to establish an investigation's scope from day one will ensure that the investigation does not get off the ground in a rudderless fashion, even if the scope must ultimately be adjusted as new facts emerge.

The scope of the investigation will depend on the investigation's triggering event. For instance, if the investigation is a reaction to media reports, whistleblower complaint, or internal audit finding, the scope will likely be an investigation of the allegations contained therein. If the trigger is a regulatory inquiry, the actual and expected areas of regulatory interest will determine the scope of the investigation, and it is important to discuss the regulator's expectations for the scope of the investigation early on. It may be important to have the initial investigation plan identify the specific allegations to be investigated to avoid wasteful and unnecessary "mission creep." A good rule of thumb is reflected in the Department of Justice's ("DOJ") stated expectation that companies "carry out investigations that are thorough but tailored to the scope of the wrongdoing."[1]

It is often the case that additional issues will surface when investigating facts within the original scope of an investigation. It is important, however, that any new issues are neither reflexively added to the scope of an investigation nor cast aside. Rather, new issues should be duly considered by the investigating team and the individuals overseeing the investigation to determine whether expanding the scope of the investigation is necessary or appropriate or otherwise in the best interests of the company.

[1] *Frequently Asked Questions: Corporate Cooperation and the Individual Accountability Policy)*, Dep't of Just., https://www.justice.gov/archives/dag/individual-accountability/faq (last visited Aug. 2, 2018).

Determine the goals

In addition to determining the scope of the investigation in the investigative plan, it is helpful to identify the goals of the investigation. A goal of almost every investigation is to establish the underlying facts that led to the initiation of the investigation. Beyond that, the goals of an investigation can range from delivering a factual report to the individuals overseeing the investigation, providing cooperation to regulatory authorities, determining whether the company has any legal claims or liabilities, and/or identifying remedial measures for any harm suffered by the company, among other examples. Determining the goals of the investigation will help maintain focus on the intended benefits and purposes of the investigation.

Determine who will be conducting the investigation

Clearly identify who is overseeing the investigation

It must be made clear whether the investigation is being overseen by company management, the board, a regular committee of the board, or a special committee of disinterested directors. Consciously making this decision at the outset of the investigation is critical to avoiding having to redo investigatory work if it is later determined that the investigation would have been better overseen by another group.

In many cases it is perfectly appropriate for company management or the board as a whole to oversee an investigation. There is value to having an investigation overseen by company management. Company management should have the best understanding of the business and be able to direct counsel to appropriate areas of investigation, while it also has the responsibility for the business and thus can help ensure that the conduct of the investigation does not unduly interfere with the company's operations and is not unduly wasteful. However, if there is a reason to believe that a current member of management or the board is implicated in the subject matter of the investigation, or otherwise has a conflict, it may be advisable for a special committee of the board to be established to oversee an independent investigation. Moreover, there may be other advantages to having an independent investigation, even when there is no clear conflict, including that regulators and other stakeholders may view the investigation's findings as more objective and credible. Setting up such a special committee may require hiring counsel that is separate from the company's regular counsel in order to prevent a potential conflict or appearance

of conflict. Even if a special committee is not established, in no circumstances should an officer, director, or other employee potentially involved in misconduct be responsible for overseeing or conducting an internal investigation. A real or perceived conflict of interest can undermine the integrity of the investigation and affect its credibility in the eyes of the various stakeholders, including regulators, shareholders, employees, and the public.

Identify who the investigators will be

In addition to identifying the body overseeing the investigation, it is also important to determine at the outset who the primary investigators will be. Although there may be some flexibility in adding to an investigative team at a later stage, it is often preferable to choose the primary investigators at the initial stages to ensure consistency and efficiency.

In-house. The advantages of using in-house investigators include insider knowledge and perspective of the company, as well as lower costs for conducting the investigation. This is often a viable option when the investigation is sufficiently contained, does not involve high-level executives, there are adequate in-house resources available to investigate the issues fully without it becoming a disproportionate distraction for company personnel, and when regulator interaction is not anticipated. In-house investigators can also be utilized when there is no reason to conduct an independent investigation. In all such cases, the investigation should be overseen by in-house lawyers to ensure the maximum privilege protection, even if in-house counsel utilizes non-lawyers to conduct certain investigatory tasks at their direction.

In larger investigations, or investigations that are particularly significant or time-sensitive, it will often be preferable or necessary to retain outside counsel. It is important to choose outside counsel that has both the resources and expertise to conduct a credible investigation.

Outside counsel will also often have the ability to leverage its resources to complete the investigation in an expeditious manner to prevent the investigation from lingering over the company and draining internal resources for months or even years. Moreover, when there is the possibility of regulator interest, regulators often expect significant investigations to be conducted by outside counsel. Outside counsel also

often deal with regulators across several matters, resulting in productive working relationships and credibility that can be important when advocating on the company's behalf. Further, outside counsel can manage a globally-coordinated response when regulators in multiple jurisdictions are involved. Finally, utilizing outside counsel can be helpful in maintaining privilege because almost all substantive work and communications by outside counsel will be presumptively privileged, while in-house counsel will on occasion be involved in non-legal related issues in their day-to-day roles. Indeed, in some jurisdictions, communications with in-house counsel are not privileged at all.[2]

Consultants and experts, if necessary. Some internal investigations require accounting, forensic, technical, and/or data analysis experts or consultants.[3] To ensure maximum privilege protection, counsel conducting the investigation should hire all experts or consultants.[4] In order to preserve privilege, ensure that expert and consultant engagement letters are drafted to expressly memorialize that the communications to and from the expert/consultant will be made in confidence and for the purpose of obtaining or providing legal advice.[5]

Timeline

Many factors determine the timing for an investigation, such as the nature of the investigation and the investigation trigger, which may determine how quickly the investigation can or must be conducted. Some investigations can take a matter of days, while others will last a year or longer. Where possible, setting at least tentative timing goals for an investigation's initial stages will help the investigative team stay focused on acting with deliberate speed and set expectations for those overseeing the investigation. Complex investigations may require multi-stage and/or staggered investigative phases, so it is important to identify the highest priority work-streams. If regulatory bodies are already involved, discuss with them their progress and

---

[2] For further discussion, *see* Chapter IV: Preserving Legal Privilege.

[3] Communications with these experts can be covered by attorney-client privilege. Four factors must be met in order to trigger attorney-client protection between the company and these third party experts under U.S. law. *See* Chapter IV: Preserving Legal Privilege).

[4] *United States v. Kovel*, 296 F.2d 918, 921-22 (2d Cir. 1961). *Kovel* holds that attorney-client privilege extends to communications an attorney has with an outside expert if those communications are made in confidence for the purpose of obtaining legal advice from the lawyer (*e.g.,* consulting an accountant to understand underlying financial documents in order to render a legal opinion). *Id.*

[5] *See id*.

timing expectations. In some cases, statutes of limitations, tolling agreements, auditor needs, or related parallel civil litigation, can also affect timing.

Gathering Background Facts

After establishing an investigative plan, the first stage in an internal investigation is often the gathering of background information from the individuals knowledgeable of the basic underlying facts at issue. Some of these background facts may also be gathered even before the investigative plan is finalized and will be useful in formulating the investigative plan.

This stage involves informal interviews with company personnel who are not necessarily firsthand witnesses to the conduct at issue, but have received enough information to convey to the investigators what is believed to have occurred and/or general knowledge concerning the impacted area. In addition to getting a basic understanding of what should be investigated, this initial stage should be focused on identifying the individuals who are likely to have key information and documents.

For example, if misconduct is believed to have occurred in a particular department of a company, initial background information may be gathered from one or more supervisors in that department who, in addition to having information about the facts to be investigated, will be familiar with the general workings of the relevant group as well as the key relevant employees. As another example, if the investigation concerns a whistleblower report, investigators may first interview the internal audit personnel or other employee who initially received the whistleblower report. In other cases, the background information may be gathered from in-house counsel who have learned the basic facts by being part of the initial response team. In most cases, and wherever possible, the initial background information should not be gathered from witnesses directly implicated in any relevant misconduct, so that investigators can gather as much information as possible before interviewing and evaluating the information provided by key witnesses.

Document Preservation, Collection & Review

The next stage in a typical internal investigation is document preservation, collection, and review.

Identify Document Custodians

The identification of the initial set of custodians is often done through the background fact gathering described above. It may also be helpful to consult relevant organizational charts and documents relevant to the investigation (if available) to identify relevant custodians. Care frequently should be taken to ensure the custodian group is broad enough to satisfy expectations of regulators, auditors, or other external constituents, as appropriate.

Preservation of Documents

After identifying all of the custodians who are likely to have relevant documents, a company should take steps to preserve any such documents for the relevant timeframe. The first step for preservation is to identify the types of information that may exist. This often includes electronic data stored on servers, local drives, smartphones, and shared databases, among other sources. Other types of potentially relevant files include paper documents that would not have been captured in the electronic collection and special types of data, such as recorded phone calls or transaction data. Take a broad view at the identification stage, for example, by potentially including documents held by assistants of key individuals, off-site storage locations, or home office computers.

Preservation may be done by issuing written document hold notices to employees and/or the company taking its own steps to preserve centrally stored documents, including electronic data. When available, the latter method is often used to ensure that employees do not inadvertently or intentionally destroy relevant information, as well as in situations where a company does not yet want to reveal to employees that it is conducting an investigation.

Prompt and thorough preservation of documents is critical for any investigation, both to ensure that relevant information can be reviewed and because enforcement authorities and courts take a strong negative view of any carelessness or intentional conduct that leads to the spoliation of evidence.

Collect Potentially Relevant Documents

The next step is to determine a collection protocol. For electronic data, determine the forensic collection method, including whether it can be done with in-house personnel, such as members of the company's IT department, or if an outside firm will be required. Maintain a record of the chain of custody. Files can be difficult to track back to their original locations afterwards if not done properly from the outset. Additionally, many regulators require certain metadata to be produced and retained. Another consideration is that documents will often need to be searchable by categories like subject, custodian, and email fields once they are included in a review platform.

Review Protocol

Once documents are collected from electronic and other sources, they should be reviewed pursuant to a written review protocol, particularly if there is a voluminous amount of documents. The protocol should lay out how potentially relevant documents will be initially identified (through the use of electronic keywords or otherwise), how the documents will be categorized by the initial reviewers, and what information will be elevated for further review by more senior investigators.

Another key part of many review protocols is a method for identifying potentially privileged documents. For example, the review protocol may provide a list of relevant internal and external counsel, so that reviewers can identify potentially privileged communications in order to make a determination as to whether certain communications are actually privileged. Not having a rigorous privilege review can lead to the inadvertent production of privileged documents to government authorities and litigation adversaries and, in some cases, even a waiver of privilege. Keep in

mind that some privileges that exist in the U.S. might not apply in foreign countries or in foreign investigations.[6]

Further Logistical Considerations

There are several additional logistical considerations to keep in mind regarding document collection and review. It is important to consider subsidiaries or related foreign entities of the company. Depending on the scope of the request, and subject to considering potential jurisdictional issues and blocking statute issues, it may be necessary to include appropriate documents from those entities in the collection and review. If many documents are in a foreign language, anticipate a system for efficient document translation, sharing, and review by all interested parties.

As noted, investigators should also consider the impact of any data privacy laws on how documents are collected, reviewed, and produced. For example, some jurisdictions forbid personal information from being sent out of the jurisdiction absent certain circumstances. This may counsel or even require the review of certain information within the physical jurisdiction. Some jurisdictions do not allow cooperation with foreign authorities and have enacted blocking statutes that limit or bar the production of documents and information for use in foreign litigation. Those blocking statutes, however, usually permit a work-around, such as requesting those materials through the Hague Evidence Convention, but additional time must, accordingly, be factored into the process.[7]

Conducting Interviews[8]

The next stage of an internal investigation is often interviewing fact witnesses. Once the document collection and review process has identified important documents and the key individuals, interviews should be conducted to learn more about the issues being investigated and to understand the salient events and evidence.

---

[6] *See* Chapter IV: Preserving Legal Privilege.

[7] *See* Chapter V: Data Privacy & Blocking Statutes.

[8] For more information concerning interviews, *see* Chapter IV: Preserving Legal Privilege and Chapter V: Data Privacy & Blocking Statutes.

Representation Issues

Determine if the witness already has individual counsel

When conducting witness interviews, determine if the witness has hired individual counsel. Representation will impact the way the interview is conducted and could implicate privilege issues when sharing documents with witness counsel. Note that for multi-jurisdictional investigations, employees who are based outside of the U.S. might also have individual counsel from their country of residence.

Determine whether individual counsel is needed

Where the witness does not already have individual counsel, investigators should determine whether individual counsel is advisable. Individual counsel is likely advisable when a conflict of interest exists between the company and the employee.[9] A conflict of interest does not require opposite interests and exists any time there is divergence in the interests of the company as compared to those of the employee. There are several ways that conflicts of interest may arise during the course of an investigation.[10]

Lawyers representing the corporation generally should inform the corporation's employees that they represent the corporation and not individual employees (so-called "*Upjohn*" warnings named after a U.S. Supreme Court decision).[11] The failure to give a warning may create obstacles to sharing the information obtained in the interview, particularly if the witness is left with the impression that company counsel is representing the individual. When giving warnings, lawyers should further inform the employees that the conversation is privileged, but that the privilege belongs to the corporation, which can waive the privilege at its discretion.[12] Such

[9] The Model Rules of Professional Conduct impose limits on an attorney's transactions with an unrepresented witness, including that the attorney should not state or imply that she is disinterested, must correct an unrepresented person's misunderstanding regarding the attorney's role in the matter, and may not provide advice except where the witness has a conflict with the company, that the unrepresented witness should secure counsel. Model Rules of Prof'l Conduct r. 4.3 (Am. Bar Ass'n 2018). Further, where the company's counsel knows or should know that the organization's interests are adverse to the employee's interests, the company's counsel must explain that they represent the company and not that employee. *Id*. at § 1.13(f).

[10] *See also* Chapter VI: Employee Rights & Privileges.

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

[12] *See* Chapter IV: Preserving Legal Privilege.

warnings are helpful in ensuring that privilege is maintained.[13] Interviews should then be properly memorialized to show that the warnings were conveyed.[14]

If the company has determined that a potential interviewee was likely involved in criminal misconduct, there is likely a conflict between the company and the employee, particularly if the company is cooperating with prosecuting authorities. This is true because the employee might want to invoke his or her Fifth Amendment Right not to self-incriminate, while the company has incentive to encourage the employee to speak. Potential criminal misconduct, however, is not required, and conflicts can arise when the employee has any potential civil liability, has engaged in any conduct that could be actionable by the company through disciplinary measures, or any time the individual is under investigation by the company.[15] Finally, conflicts can arise at any time, even once a company has already decided to represent an employee.

Interview Best Practices

Best practices for preparing an interview outline

While preparing an interview outline, review documents authored by the witness, collected from the witness, that mention the witness, or that contain subject matter pertinent to the witness (such as internal company policies or documents available company-wide). You may also ask about any communications on which the witness was copied even if he or she was not the sender. You will also wish to incorporate any information learned about the witness through prior interviews.

Consider preparing questions to: (1) learn facts (both to understand what you think you know and what you do not know); (2) identify other potential witnesses; (3) identify other relevant documents; (4) test legal theories; and/or (5) explore

[13] An employee can prove that an attorney-client relationship was formed by showing that their subjective belief of the formation of an attorney-client relationship was reasonable under the circumstances. *In re Grand Jury Subpoena: Under Seal*, 415 F.3d 333, 339 (4th Cir. 2005), *cert. denied*, 546 U.S. 1131 (2006). If that employee can show the formation of an attorney-client relationship with company counsel, then the employee will be able to determine whether privilege can be waived, and, in the event of conflict between company and employee, company counsel would need to withdraw from all representation to maintain all confidences. *See id*. at 340; *see also* Model Rules of Prof'l Conduct r. 1.13(f) (Am. Bar Ass'n 2018).

[14] For more information on note taking *see* Chapter IV: Preserving Legal Privilege.

[15] *See* Model Rules of Prof'l Conduct r. 1.7 (Am. Bar Ass'n 2018); *see also Upjohn Co.*, 449 U.S. at 383; *In re Grand Jury Subpoena: Under Seal*, 415 F.3d at 340; *United States v. Keplinger*, 776 F.2d 678, 701 (7th Cir. 1985) (discussing whether company counsel represented employees and implications on privilege).

potential biases of the witness. Be prepared to ask fact witnesses about all important topics, even if just to confirm that the witness knows nothing about some of them.

If the company and individual counsel are engaged in a cooperative relationship, consult with the individual counsel to determine what information might have been learned previously and share documents that will be discussed at the interview ahead of time to ensure a productive interview—just remember to be cognizant of privilege issues. In cross-border matters, also consult with co-counsel in other jurisdictions and individual counsel to determine the most strategic and appropriate approach to the interview.

Best practices during and after the interview

Bring all relevant documents to the interview and, in the case of documents translated from their original language, make sure to have copies of documents in both the original and translated language.

Consider only including attorneys and paralegals in the interview and designating one person to take notes and write an interview memorandum. Limiting attendance also helps witnesses to speak more openly. Always check beforehand whether the interviewee would prefer to conduct the interview in their native language and have an interpreter available.

If the interview will be conducted in multiple languages using an interpreter, be prepared for the interview to take considerably longer and plan accordingly. In some circumstances, if the witness will be bringing an interpreter, you may want to bring your own interpreter to confirm that the translation is accurate. Even if the employee is comfortable conducting the interview in English, an interpreter should be available to confirm any discrepancy in translations that could affect substantive understanding.

A final consideration is to make sure to show witnesses only documents that they would have seen at the time; this will avoid leading witnesses to speculate on matters they were not involved with. For example, if the witness was only included on earlier emails in an email chain, consider redacting the portions the witness would not have seen at the time when showing the document. Similarly, interviewers should

not otherwise educate fact witnesses about important facts and events of which the witness is not otherwise aware.

Interview memos should be prepared to record and summarize the substantive information that was learned from the interview so that the information can be accessed at a later point in time. Be sure to make clear that the memoranda are not verbatim transcripts and include the author's thoughts and mental impressions in order to maintain privilege.[16] The interview memorandum should be finalized shortly after the interview is complete while the events and mental impressions of the writer are still fresh.

Reporting: Disclosing the Investigation Results

Format of Reporting

The company should consider its goals, objectives, and audience when determining whether to deliver the results of the investigation orally, in a written report, or with a presentation. A lengthy written report will provide the company a comprehensive record of the investigation and its methodology and findings, but it can create potential litigation risk in the future and may be an inefficient mechanism for conveying information; a set of PowerPoint slides, however, may convey the most important information and serve as a useful record of the investigation, but it will sacrifice detail. A further alternative is for counsel to make an oral report and to keep a record in its files of what the investigation looked at and found.

Audience

To Management and/or the Board

Companies should consider early on who will get the results of the investigation and in what format. For a lengthy investigation, senior management or the board may want periodic updates, particularly to the extent it impacts daily business decisions for the company while the investigation is ongoing.[17]

[16] *See* Chapter IV: Preserving Legal Privilege.

[17] For more information on privilege issues when the client is the company as compared to a particular committee, *see* Chapter IV: Preserving Legal Privilege.

To Regulators

When companies are faced with a regulatory investigation, they often choose to cooperate with the regulators. In the course of such cooperation, the results of the investigation will likely be shared with the relevant regulators through several formats and over a period of time. This can include any combination of document productions, proffers, presentations, and making witnesses available for interviews. The goal of presentations is to demonstrate the company's commitment to cooperation, by assisting the regulators in their own investigations, while at the same ensuring that all relevant information is provided and considered before any regulatory action is taken.

CASE STUDY:
HERRERA

Internal and external lawyers should carefully consider their approach when conducting internal investigations, particularly when providing downloads to the government of material that may be privileged or subject to work product protection. In *SEC v. Herrera*, an oral download of external counsel's interview notes to the Securities and Exchange Commission ("SEC" or "Commission") was considered to have waived protection from disclosure under the attorney work product doctrine, and the law firm that presented the proffer was ordered to disclose the notes that were orally downloaded.[18]

Privilege Waiver

It is occasionally in a company's interest to disclose the results of its investigation either to the authorities, to the broader public, or to some narrower external constituency such as auditors or underwriters in a public offering. During the course of disclosing investigation results to authorities or external constituencies, there will likely be considerations regarding privilege waiver. With respect to governmental authorities, in theory, failure to waive privilege should not impact cooperation credit, but in practice the question is more nuanced.

Relevant information collected during the investigation is expected to be disclosed by a company in a cooperative relationship with the government. The failure to

[18] *SEC v. Herrera*, 324 F.R.D. 258, 264-67 (S.D. Fla. 2017).

disclose relevant information can impact the outcome of the case.[19] For this reason, the decision to participate in any joint defense agreement with an individual or other company should be carefully considered, and any such agreement should be carefully crafted to provide flexibility for the company. While joint defense agreements themselves do not impact eligibility for cooperation credit, such an agreement could limit the company's ability to seek maximum cooperation credit if a situation arises where the company is prevented from producing privileged material favorable to it.[20] One question the company might carefully consider is whether to enter into a joint defense agreement with counsel for one of its executives or employees. While such an agreement might facilitate the transfer of information and enhance the company's ability to make accurate and fair findings, it could also constrain the company's ability to share information obtained from the individual with the government, unless the agreement is carefully drafted.

If the company decides to provide the results of its investigation to the government, it should be mindful of the impact such cooperation could have on the company's ability to invoke privilege and withhold such information in subsequent enforcement actions or civil litigation. In a cooperative posture with the government, the company can suggest methods of providing such documents that would prevent them from being discoverable in a later action. An example of such a strategy would be to confirm any information is grand jury material under Fed. R. Crim. P. 6(e) (so they are exempt from production) or to enter into a non-disclosure agreement.[21]

Care should also be taken when sharing information about an investigation with the broader public, auditors, or underwriters in a public offering. Any time materials that would otherwise be protected by attorney-client privilege are voluntarily shared with a third party, the privilege is put at risk as to that communication and other communications of the same subject.[22] Documents provided to underwriters'

---

[19] For example, when using an advice of counsel defense, if an argument is being made that employees acted in good faith, showing communications where employees sought advice of in-house counsel may be crucial to a company's defense.

[20] Dep't of Just., *U.S. Attorneys' Manual* § 9 28.730 (Nov. 1997) ("USAM").

[21] *See also* Chapter IV: Preserving Legal Privilege; *see* Order, *SEC v. Bank of Am. Corp.*, No. 09 Civ. 6829 (S.D.N.Y. Oct. 14, 2009), ECF No. 33 (finding that under Rule 502(d) of the Federal Rules of Evidence, which empowers a court to determine the scope of privilege waiver for documents produced in that court, Bank of America could waive attorney-client and work-product privileges with regard to certain categories of information for the government and related state and federal inquiries without waiving those protections for other information that might be sought in related private lawsuits).

[22] *See, e.g., Weil v. Inv./Indicators, Research & Mgmt., Inc.*, 647 F.2d 18, 24 (9th Cir. 1981) ("[I]t has been widely held that voluntary disclosure of the content of a privileged attorney communication constitutes waiver of the privilege as to all other such communications on the same subject." (collecting cases)).

counsel or to another party in a transaction, for example as part of due diligence, may be considered to have been disclosed to third parties, regardless of the type of confidentiality agreement in place or sharing necessity based on due diligence obligations, and therefore constitute a waiver of attorney-client privilege.[23]

Likewise, disclosure to independent auditors is considered a waiver of attorney-client privilege in many jurisdictions. One potential solution, particularly where the auditors require certain information about an internal investigation to render an opinion, is to provide the necessary information to auditors by providing documents that are covered by work product privilege. The work product privilege, which prevents discovery of materials prepared by a party, its counsel, or other representatives in anticipation of litigation, is not automatically waived by any disclosure to a third party.[24] Instead, privilege is not waived for documents protected by work product privilege unless they are disclosed or risk being disclosed to an adversary.[25] A majority of courts have held that disclosing work product to independent auditors does not constitute a waiver because the independent auditor is not considered an adversary. This determination, however, must be made on a case-by-case basis, taking into consideration the information conveyed to auditors, the manner by which that information is conveyed, and the relevant privileges that apply to the documents at issue, as well as the case law in the relevant jurisdictions.[26]

Potential Responsive Actions

Remediation

In concluding an investigation, management, the board, the auditors, shareholders, and/or regulators will inquire as to steps the company has taken, and will continue to take, to remediate the cause of the misconduct. The DOJ in particular has taken a standard approach to evaluating the sufficiency of a company's corporate

[23] *See In re John Doe Corp.,* 675 F.2d 482, 489 (2d Cir. 1982) ("Federal securities laws put a price of disclosure upon access to interstate capital markets. Once materials are utilized in that disclosure, they become representations to third parties by the corporation. The fact that they were originally compiled by attorneys is irrelevant because they are serving a purpose other than the seeking and rendering of legal advice.").

[24] *See* Fed. R. Civ. P. 26(b)(3); *see also* Chapter IV: Preserving Legal Privilege.

[25] *See, e.g., In re Steinhardt Partners L.P.*, 9 F. 3d 230, 235 (2d Cir. 1993); *Brown v. NCL (Bahamas), Ltd.*, 155 F. Supp. 3d 1335, 1339 (S.D. Fl. 2015); *Curto v. Med. World Commc'ns, Inc.*, 783 F. Supp. 2d 373, 380 (E.D.N.Y. 2011).

[26] For more information on formulating a disclosure strategy for auditors, *see* Elizabeth (Lisa) Vicens and Daniel Queen, *Audits and Adversaries: Making Disclosures to Your Auditors Without Waiving Your Privilege*, Cleary Gottlieb (May 1, 2017), https://www.clearymawatch.com/2017/05/audits-adversaries-making-disclosures-auditors-without-waiving-privilege/#_edn4.

compliance program by asking questions aimed at examining the program's design, the stakeholders at issue, and the resources provided to compliance overall.[27]

For remediation of underlying conduct specifically, there are several important components. First, any immediate ongoing misconduct should be halted, and, if there are bad actors within the company, appropriate action should be taken to prevent any continuing harm to the company and others. Second, a root cause analysis should be conducted to determine the root cause of the misconduct at issue and any systemic issues identified.

Remedial action can also include improving internal controls, policies and procedures, and training. Other measures could include employee discipline or severing relationships with third parties. Note that certain actions like employee discipline can be impacted by foreign labor laws.

For public companies subject to requirements under the Sarbanes-Oxley Act of 2002, deficiencies identified by management (for example, through an internal investigation) or by auditors will also require remediation. Under Section 404 of Sarbanes-Oxley, public companies must attest to the adequacy of the company's internal controls to prove compliance with the Act. Material weaknesses in a public company's internal controls that exist as of the year-end assessment date must be disclosed to the public. If such deficiencies are identified and remediated prior to that date, the company may be able to limit the public disclosure necessary, incentivizing a proactive approach to remediation.

A public company's board of directors is also required to be informed of matters that could impact the company's compliance with the law, which means that the directors must ensure the company is adequately handling risk.[28] These responsibilities are typically satisfied with a well-designed and administered compliance system, such that any material compliance issues appropriately make their way to management. In the event that an internal investigation highlights a deficiency in the compliance system or risk management, the board must remedy the area of concern in a timely

[27] *See Evaluation of Corporate Compliance Programs,* Dep't of Justice, Crim. Div., Fraud Section, https://www.justice.gov/criminal-fraud/page/file/937501/download; *see also* USAM § 9-28.

[28] *See In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 970 (Del. Ch. 1996) (finding that corporate directors' fiduciary duties to a company requires adopting and maintaining compliance programs that can adequately detect corporate wrongdoing and properly elevate those issues to the company's management and board of directors).

manner in order to protect the board's decisions from potential liability in a shareholder derivative suit if the company suffers losses due to compliance violations.[29]

Self-reporting

Although there is no general rule that a company must disclose employee misconduct, disclosure can be triggered by other reporting obligations, or a company can choose to voluntarily self-report to regulators. Regulated entities, such as reporting companies, might have their own disclosure obligations and should therefore ensure that the proper information is disclosed accordingly.

Voluntarily self-reporting can lead to reduced penalties through cooperation credit and gives the corporation the opportunity to exercise some control of how and when the information is first disclosed. However, voluntary self-disclosure also has risks, including creating regulator interest when there is none to begin with, prolonged cooperation obligations, and increased government scrutiny. Self-reporting decisions should be formulated in consultation with counsel.

Market Disclosure

Disclosure advice is frequently jurisdiction and fact specific, and beyond the scope of this Handbook. For disclosure advice, companies are usually well-advised to consult their regular disclosure counsel. Nonetheless, a few considerations are in order.

In cases of public companies, reporting obligations may trigger the disclosure of an internal investigation, but typically discovering corporate misconduct through an internal investigation, without being part of a larger trend, does not itself require public disclosure. For example, the Securities Exchange Act of 1934 generally requires that companies not make materially misleading statements. Under SEC regulation S-K Item 103, companies are required to disclose "Legal Proceedings," an obligation that is triggered when "the regulatory investigation matures to the point where litigation is apparent and substantially certain to occur," meaning that even a notification to the company that it is under investigation is not in itself necessarily

[29] *Id.; see also Stone v. Ritter*, 911 A.2d 362, 372 (Del. 2006) (finding that director liability exists where there is "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists.").

sufficient to trigger the obligation.[30] However, the company is required to disclose known trends or uncertainties that might have, or could be reasonably expected to have, a material unfavorable impact on the company's business, which includes patterns related to corporate misconduct learned through an internal investigation.[31] The determination of whether to disclose the results of an investigation will, in any event, require a careful analysis. Even if a determination is made that affirmative disclosure is not required, a company should nonetheless consider whether such disclosure might still be in its best interest.

Other Disclosures

Consideration should also be given to whether and to what degree information from the investigation requires disclosures to other external constituencies. For example, disclosure requirements could arise under Section 10A of the Securities Exchange Act of 1934, which outlines the required steps auditors must take when an illegal act has been discovered, and states that if the issue has not been remediated by the time the auditor is required to report the issue to the company's board of directors, then the company must self-report to the SEC within one business day. Otherwise, the auditor must report the issue to the SEC. Other external constituency disclosures to consider are underwriters, which might be a required part of due diligence, merger or transaction counterparties, or lenders.

Cross-Border Considerations

Cross-border investigations add additional layers of complexity to a process that already consists of many moving parts. The most important element of having an effective global strategy is communication, including frequent and efficient communication with the investigation team, those overseeing the investigation, local experts, regulators, and other stakeholders.

[30] *See, e.g., Richman v. Goldman Sachs Grp. Inc.*, 868 F. Supp. 2d 261, 274-75 (S.D.N.Y. 2012).

[31] 17 C.F.R. § 229.303(a)(3)(ii) (2018).

CROSS-BORDER CONSIDERATIONS

— Consider the laws in all jurisdictions in which the company is located, all jurisdictions in which alleged misconduct took place, and all jurisdictions in which government authorities are conducting investigations that might impact strategy and decision making.

— Engage in open communication across multiple parties to manage expectations and anticipate any issues, including with:

- Local counsel, teams conducting the investigation in different jurisdictions, and other teams working on related investigations, in order to ensure the investigation is coordinated, operating at the same pace, and relevant information is shared.
- Regulators in order to understand their expectations and ensure that all investigations are moving, to the extent possible, at approximately the same pace, as well as to inform regulators of any actions taken by a foreign governmental entity that could impact their investigation.

The subject matter of an investigation may necessitate special considerations. Below is a chart that describes some common special considerations for certain types of investigations.

EXAMPLES OF SPECIAL CONSIDERATIONS

Antitrust:

— Antitrust enforcement is growing around the world, and multinational companies are increasingly subject to simultaneous review by multiple antitrust regulators.

— Legal standards for what constitutes per se illegal antitrust activity varies significantly between jurisdictions.

Corruption:

— The nature of corruption crimes can require reverse engineering payment streams, such as through reviewing money transfer patterns. The time and resources this will take should be taken into consideration when crafting an investigative plan.

Cybersecurity:

— When investigating a potential cybersecurity incident or data breach, it is essential to establish a secure communication channel while conducting an investigation until any potential breaches have been identified.

Sexual Harassment:

— Applicable laws and policies should be evaluated from federal and state law as well as internal company policies and procedures.

— The investigation should work closely with the human resources department to ensure all relevant complaints are investigated.

— Witness and complainant interviews require sensitivity to potentially emotionally charged circumstances giving rise to the complaint.

Whistleblower:

— Due to the nature of the way the information was received, it requires special care and communication.

— It is essential that nothing is done which can be perceived as retaliation against the employee, which includes ensuring that there are no efforts to discover the identity of the whistleblower.[32]

[32] For further discussion, *see* Chapter VI: Employee Rights and Privileges.

Conclusion

While for purposes of this summary we have presented the investigation lifecycle in a linear fashion, in most cases, particularly in larger investigations, the investigative steps can overlap and cycle back several times before the investigation is completed. For example, an initial round of interviews may lead to identifying new potentially relevant documents and relevant interviewees, leading to a new round of document review and interviews, and so on. Similarly, a follow-on government request after an initial disclosure will often lead to another round (or more) of document review and interviews. Whatever the final scope and outcome of an investigation, taking a deliberative and methodical approach along the lines above will ultimately inure to the company's benefit and help achieve the objectives of an investigation.

Chapter IV:
Preserving Legal Privilege

The United States

Summary

Key Privileges:

— Attorney-Client: Protects communications with a lawyer or attorney's representative for the purposes of obtaining legal advice.

— Work Product Doctrine: Protects work product of lawyers or those acting on their behalf when prepared in reasonable anticipation of litigation.

— Other privileges or confidentiality protections may apply to self-critical analysis, bank examination, law enforcement requests, and other materials.

Protecting the Privileges:

— Voluntary disclosure of privileged materials is generally construed as a waiver of privilege.

— The waiver may extend to all privileged materials concerning the same subject matter.

— The waiver will generally not be limited to a specific party or even to specific documents, as most U.S. jurisdictions do not recognize "selective waiver."

— Other statutes or rules may prevent waiver of privilege even where it is voluntarily disclosed.

— Inadvertent disclosure of privileged materials will generally not waive the privilege as long as the disclosing party (i) took reasonable steps to prevent the disclosure, and (ii) took prompt action to rectify the error.

Introduction

U.S. law recognizes a number of legal privileges and other confidentiality doctrines that can shield documents and communications from disclosure. The most common privileges are the attorney-client privilege and the work product doctrine. These privileges protect communications with clients and the work product of lawyers prepared in reasonable anticipation of litigation. Other lesser-known privileges may protect certain other types of materials. For example, certain jurisdictions protect self-critical analysis (internal investigations) from disclosure, whether or not they involve lawyers.[1] In other circumstances, it may be possible to withhold materials from production on the basis of privileges that belong to others. The bank examination privilege, for example, entitles bank regulators—such as the CFPB, any federal banking agency, any state bank supervisor, or any foreign banking authority—to object to the disclosure of information concerning their past or ongoing bank examinations.[2]

In certain circumstances, these privileges can attach to sensitive information compiled and analyzed in the course of an internal investigation into potential wrongdoing, initiated either by the company itself, or in response to a government inquiry. Absent an exception or waiver, a company cannot be compelled to disclose privileged information or documents to most government authorities, civil plaintiffs, or any others.[3]

PRACTICE TIP:
PRIVILEGES ARE NOT ABSOLUTE

Privileges are not absolute shields. They are often narrowly construed by the courts. Be sure to follow proper procedures for preserving privilege.

[1] *See, e.g., Tice v. Am. Airlines, Inc.*, 192 F.R.D. 270 (N.D. Ill. 2000) (applying the federal common law of the self-critical analysis privilege); *Bredice v. Doctors Hosp., Inc.*, 50 F.R.D. 249, 250 (D.D.C. 1970), *aff'd*, 479 F.2d 920 (D.C. Cir. 1973) (holding that, under federal law, a hospital had a qualified privilege to doctors' critical analyses of medical care to a decedent because disclosure would deter improvements in patient treatment).

[2] *See also* Chapter II: Responding to Requests from Authorities.

[3] In certain exceptional circumstances, such as during regulatory bank examinations, it may not be possible to withhold privileged materials, but the law may afford other protections, such as providing that the production of such material does not constitute a waiver.

Privileges must be protected or they can be waived. Thus, companies must take care during the course of internal investigations and in responding to governmental requests for information:

— To manage investigations with an eye towards maintaining legal privilege over the materials.

— Not to waive any legal privileges that may apply, except where such waiver may work to the company's advantage.

In certain circumstances, a company may choose to disclose the results of its investigation and facts learned during the investigation to the government. Such disclosure of information learned by counsel in a privileged setting in the course of an investigation can result in a waiver of the privilege as to third parties. The benefits of providing investigative findings can include: (i) demonstrating cooperation in the hopes of getting credit in the context of resolving a government investigation; (ii) being able to frame the investigative facts and provide the appropriate context; (iii) in the instance in which the investigative results including findings of wrongdoing, being able to get a speedy resolution and provide the appropriate information to all external constituencies; and (iv) providing criminal and regulatory authorities with exculpatory evidence collected during an investigation. Thus—and while U.S. prosecutors and regulators generally have policies against *requiring* companies to waive privileges in an investigation in order to obtain cooperation credit—sharing information obtained in an investigation may nonetheless be in the company's interest and benefit the company's posture with the government.

Ultimately, however, a company responding to government inquiries needs to make sure that any disclosure of information that may result in a waiver is an informed one, not something foisted upon it because it was not sufficiently vigilant to maintain its privileges during the course of that investigation.

PRACTICE TIP:
THE RISKS OF PROVIDING PRIVILEGED INVESTIGATIVE INFORMATION TO THE GOVERNMENT

Providing investigative information to the government, particularly voluntarily, creates a number of potential risks.

— The provision of information may result in a waiver as to third parties, including investigation by a different regulator or a subsequent civil litigation.

— The company may find it difficult, if not impossible, to cabin its waiver. In other words, it is difficult to waive a privilege for some purposes but retain the privilege for other purposes.

— Likewise, in most jurisdictions, the waiver of privilege with respect to certain privileged materials may be construed as waiver of privilege with respect to all materials concerning the same subject matter.

What law will apply?

In the cross-border context, it is important to assess what substantive law of privilege may govern a dispute. In the United States, each state and the federal government has their own privilege law. Foreign jurisdictions will also have their own privilege rules, some of which will be explored later in this chapter.

Where more than one substantive law may apply, and where the outcome of the dispute would differ depending on the law that is applied,[4] courts typically conduct a choice-of-law analysis. While courts in different jurisdictions may approach the issue using slightly different tests, under the typical analysis a court will "defer[] to the law of the country that has the 'predominant' or 'the most direct and compelling interest' in whether those communications should remain confidential, unless that foreign law is contrary to the public policy of this forum."[5] This analysis primarily focuses on (i) where the communication took place; (ii) where the attorney and where the client are located; (iii) where the attorney-client relationship was entered into or where it was centered when the communication took place; and (iv) where

[4] *See Berg Chilling Sys., Inc. v. Hull Corp.*, 435 F.3d 455, 462 (3d Cir. 2006) (Alito, J.) ("According to conflicts of laws principles, where the laws of the two jurisdictions would produce the same result on the particular issue presented, there is a 'false conflict,' and the Court should avoid the choice-of-law question.").

[5] *Astra Aktiebolag v. Andrx Pharm., Inc.*, 208 F.R.D. 92, 98 (S.D.N.Y. 2002); Restatement (Second) of Conflict of Laws § 139 (1971).

the proceeding is pending.[6] Applying this rule, at least one court has held that communications made in a foreign forum without privilege protections will be admitted in the United States, even if they otherwise would have been protected were U.S. law applied.[7] Moreover, state courts generally favor admissibility and, absent some special reason, will apply the less restrictive rule between the forum state and the state with the most significant relationship with the communication.[8]

CASE STUDY:
ASTRA AKTIEBOLAG V. ANDRX PHARMACEUTICALS
UNDERSTAND THE RELEVANT FOREIGN LAW

In some circumstances, even when foreign law does not recognize a privilege, there may be an argument that a communication is protected from disclosure for other reasons. For example, in *Astra*, even though Korean law applied and did not recognize attorney-client privilege, the U.S. court nonetheless prohibited disclosure because Korean law would not permit disclosure of the document under its limited civil discovery rules. Thus, the *Astra* Court found that requiring disclosures—although not prohibited by local law—"would violate principles of comity and would offend the public policy of this forum."[9]

What are the privileges?

There are two core legal privileges in the United States:

— ***Attorney-client privilege***, for communications between clients seeking and receiving legal advice and their attorneys.

— ***Work product doctrine***, for documents prepared by or for a client in reasonable anticipation of litigation or other legal proceedings.

---

[6] *Astra*, 208 F.R.D. at 98.

[7] *See In re Rivastigmine Patent Litig.*, 237 F.R.D. 69, 76 (S.D.N.Y. 2006) (rejecting privilege claims under Swiss law, which, unlike U.S. law, does not create privilege for communications with in-house counsel), *aff'd in relevant part*, 239 F.R.D. 351, 356-59 (S.D.N.Y. 2006); *cf. Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 66-67 (S.D.N.Y. 2010) (applying U.S. privilege law even to communications made in Italy, because the communications concerned U.S. litigation over U.S.registered trademarks).

[8] *See, e.g., Major v. Commonwealth*, 275 S.W.3d 706, 714 (Ky. 2009) (citing Restatement (Second) of Conflict of Laws § 139 (1988)); *People v. Allen*, 784 N.E.2d 393, 395-96 (Il. App. Ct. 2003) (applying less restrictive rule); *Kos v. State*, 15 S.W.3d 633, 638-40 (Tex. App. 2000) (same); *State v. Eldrenkamp*, 541 N.W.2d 877, 881 82 (Iowa 1995) (same).

[9] *Astra*, 208 F.R.D. at 102.

There are a number of other privileges and protective doctrines—including common interest privilege, self-critical analysis privilege, and bank examination privilege—that can also shield company documents from production to governmental authorities or civil litigants. Those will be addressed, as relevant, below.

Attorney-Client Privilege

The attorney client privilege protects certain communications between attorneys and their clients from compelled disclosure. It is intended to promote open communications between attorneys and their clients.[10]

ELEMENTS:
ATTORNEY-CLIENT PRIVILEGE

To be privileged, communications must be:

— Between a client and her attorney.[11]

— Intended to be, and were, kept confidential.

— Made for the purpose of obtaining or providing legal assistance.[12]

[10] *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

[11] Note that the "general rule under United States law is that only communications between a represented party and that party's licensed attorneys are subject to attorney-client privilege." *Anwar v. Fairfield Greenwich Ltd.*, 982 F. Supp. 2d 260, 265 (S.D.N.Y. 2013); *see also A.I.A. Holdings, S.A. v. Lehman Bros., Inc.*, No. 97 Civ. 4978(LMM)(HB), 2002 WL 31385824, at *4 (S.D.N.Y. Oct. 21, 2002), *supplemented sub nom. A.I.A. Holdings v. Lehman Bros., Inc.*, No. 97 Civ. 4978 (LMM)(HB), 2002 WL 31556382 (S.D.N.Y. Nov. 15, 2002) ("[T]he attorney must actually be admitted to the bar of a state or federal court [except]. . . . in the absence of an excusable mistake of fact.") (internal quotations omitted). However, if a client has a "reasonable belief" that an individual is a licensed attorney—for example, if that individual held herself out as an attorney or performed acts suggesting she is an attorney—communications between the client and the non-licensed attorney may be found to be protected by the attorney-client privilege. *See Anwar*, 982 F. Supp. 2d at 265; *see also Gucci Am., Inc. v. Guess?, Inc.*, No. 09 Civ. 4373 (SAS), 2011 WL 9375, at *5 (S.D.N.Y. Jan. 3, 2011) (holding that the well-established "reasonable belief" exception applies to both individuals and corporations alike).

[12] *See Brennan Ctr. for Justice at N.Y. Univ. Sch. of Law v. U.S. Dep't of Justice*, 697 F.3d 184, 207 (2d Cir. 2012).

Who controls the attorney-client privilege?

The attorney-client privilege belongs to—and must be asserted by—the client.[13] Attorneys and their agents cannot disclose information subject to the privilege without client permission.[14] On the other hand, where a client consents to disclosure of privileged information or communications, there is no independent basis on which the attorney can object to disclosure.[15] Within companies, where the privilege belongs to the company and not to its individual employees, the decision whether to permit disclosure generally lies with officers and directors.[16]

How does the attorney-client privilege apply in the corporate context?

Because the client in this context is an entity, and not any one individual, corporations and their attorneys must be careful to ensure that communications with various employees will benefit from the protections of the attorney-client privilege. Communications with different agents and employees of the corporation are subject to different privilege rules.

Outside counsel. The attorney-client privilege originated in circumstances surrounding communications with outside counsel. As such, communications with outside counsel for the purpose of obtaining legal advice are generally protected so long as they otherwise meet the elements of privilege.[17]

Agents of counsel. Sometimes companies and counsel will determine that it is necessary to retain third-parties in order to assist with specialized aspects of an internal investigation. For example, counsel may hire a forensic accountant to examine the company's books and records, or an expert, such as an engineer, to determine compliance with government regulations. Communications involving clients and these agents of counsel can also be privileged if they are carrying out

[13] *In re Sarrio, S.A.*, 119 F.3d 143, 147 (2d Cir. 1997).

[14] *See Swidler & Berlin v. United States*, 524 U.S. 399, 410-11 (1998).

[15] *Republic Gear Co. v. Borg-Warner Corp.*, 381 F.2d 551, 556 (2d Cir. 1967) ("an attorney [cannot] invoke the privilege for his own benefit when his client desires to waive it").

[16] *Commodity Futures Trading Comm'n v. Weintraub*, 471 U.S. 343, 348-49 (1985); *United States v. Wells Fargo Bank N.A.*, No. 12 Civ. 7527 (JMF), 2015 WL 3999074, at *2 (S.D.N.Y. June 30, 2015) (holding that, where an employee does not have the authority to waive a corporation's privilege, the invocation of an advice-of-counsel defense by that employee does not cause a waiver of the corporation's privilege).

[17] *See Gucci Am.*, 271 F.R.D. at 71.

their work at the direction of legal counsel.[18] However, it is important to ensure that the agents are performing functions fundamental to the provision of legal advice.[19] It is also important to ensure that counsel are overseeing and directing work done by their non-attorney agents and it is helpful if the agents are actually retained by counsel even if the company is paying the costs and fees of the agents. In contrast, if the agent is not employed for the specific purpose of assisting counsel in providing legal advice, the attorney-client privilege may not extend to communications with the agent.[20]

CASE STUDY:
IN RE GRAND JURY SUBPOENAS
RETENTION OF PUBLIC RELATIONS AGENTS

Often, in the midst of a crisis, a party will retain a public relations firm to help manage the situation.[21] For example, in *In re Grand Jury Subpoenas,* when the U.S. Attorney's Office for the Southern District of New York brought charges in a high profile, sealed case against a target, the target of the investigation hired a public relations firm to "affect[] the media-conveyed message that reached the prosecutors and regulators responsible for charging decisions in the investigations concerning [the] [t]arget."[22] In finding the communications among the public relations firm, the target, and the target's counsel to be protected by the attorney-client privilege, the court held that: "(i) confidential communications (ii) between lawyers and public relations consultants (iii) hired by the lawyers to assist them in dealing with the media in cases such as this (iv) that are made for the purpose of giving or receiving advice (v) directed at handling the client's legal problems are protected by the attorney-client privilege."[23] The court further noted that an important factor is whether the lawyer or the client hired the outside public relations firm; only if the lawyer hires the outside public relations firm does the attorney client privilege apply.

[18] *See United States v. Kovel*, 296 F.2d 918, 920-23 (2d Cir. 1961) (client communications with non-lawyer accountant employee of law firm considered privileged); *In re Grand Jury Subpoenas Dated Mar. 24, 2003 Directed to (A) Grand Jury Witness Firm & (B) Grand Jury Witness*, 265 F. Supp. 2d 321, 325-30 (S.D.N.Y. 2003) (client communications with public relations firm hired by law firm considered privileged); *Gucci Am.* 271 F.R.D. at 71 (communications with investigators working for counsel privileged).

[19] *Cavallaro v. United States*, 284 F.3d 236, 247 (1st Cir. 2002) ("The communication, however, must be made 'for the purpose of obtaining legal advice from the lawyer.' ' If what is sought is not legal advice but only [other] service. . .or if the advice sought is the [non-lawyer's] rather than the lawyer's, no privilege exists.'"); *see also United States v. ChevronTexaco Corp.*, 241 F. Supp. 2d 1065, 1072 (N.D. Cal. 2002) (communications with accountant were not privileged where accountant provided his or her own additional advice about the client's situation); *Kovel*, 296 F.2d at 922.

[20] *See Cavallaro*, 284 F.3d at 240.

[21] *See* Chapter VIII: Public Relations & Message Management.

[22] *In re Grand Jury Subpoenas*, 265 F. Supp. 2d at 323-24.

[23] *Id*. at 331.

In-house counsel. In the United States, the attorney-client privilege applies with equal force to communications between the corporate client and in-house counsel.[24] However, for the privilege to attach, communications with in-house attorneys must be for the purpose of obtaining or providing legal advice. Thus, because business communications do not become privileged simply because an attorney is included in them, analyzing privileged communications involving in-house lawyers who wear dual hats may be complicated. Even then, in-house counsels' communications may not be privileged in all jurisdictions outside of the United States.[25]

CASE STUDY:
FOREIGN LAW MAY NOT PROTECT COMMUNICATIONS WITH IN-HOUSE COUNSEL

Corporations must be cognizant of whether communications that would normally be privileged in a U.S. action may not be treated as such because they occurred outside of the U.S. For example, in *Wultz v. Bank of China Ltd.*, the court found that there was no privilege because "there are cognizable distinctions between a 'lawyer' and an 'in-house counsel' in Chinese law."[26] Further, "[b]ecause Chinese law does not recognize the attorney-client privilege or the workproduct doctrine, BOC must produce those items listed on its privilege log which are governed by Chinese privilege law."[27]

Corporate employees. Communications between counsel and employees of the company are protected in certain circumstances, but the privilege is not absolute. The leading case on this topic is *Upjohn Co. v. United States*, 449 U.S. 383 (1981), in which the Supreme Court stated that communications between legal counsel and employees are protected from disclosure to third parties when:

— The information is necessary to supply the basis for the requested legal advice.

— The information concerns a matter within the scope of the employee's duties.

[24] *Upjohn*, 449 U.S. at 392-94.

[25] *See, e.g., Rivastigmine*, 237 F.R.D. at 76 (describing how Swiss law does not privilege communications with in-house counsel).

[26] *See Wultz v. Bank of China Ltd.*, 979 F. Supp. 2d 479, 495 (S.D.N.Y. 2013), *on reconsideration in part*, No. 11 Civ. 1266 (SAS), 2013 WL 6098484 (S.D.N.Y. Nov. 20, 2013).

[27] *Id.* at 493.

— The employee is aware that they were being questioned to secure legal advice for the company.[28]

Given these principles, company counsel should take care to interview employees who have knowledge necessary to an investigation. In addition, distribution of privileged documents should be limited to employees in a "need to know" position in order to not violate the "confidential" element of the attorneyclient privilege.[29] And, when interviewing employees, make sure that they know they are being interviewed to secure legal advice for the company and that the company considers the interview to be confidential and to be subject to the company's attorney-client privilege.

PRACTICE TIP:
UPJOHN, THE "CORPORATE MIRANDA" WARNING

Employees should be given a so-called *Upjohn* warning (also known as "corporate Miranda") informing them that: (i) the interviewing attorney is counsel for the company, not the employee; (ii) the company alone can choose to assert or waive the privilege, with no warning to the employee; and (iii) the employee should keep the conversation confidential in order to preserve the privilege. In addition to ensuring that the attorney-client privilege is not broken by the interviewee's disclosure of the conversation, the *Upjohn* warning also prevents formation of an individual attorney-client relationship between the lawyer and the interviewee, through which the interviewee could preclude the company from disclosing the discussion.[30]

Counsel need not always be present during a privileged communication for privilege to attach. For example, if counsel requests that a group of employees (e.g., the human resources department) gather facts in anticipation of litigation, communications among the employees regarding that request may be privileged even if counsel is not actually present.[31] Note, however, that outside of this limited exception employees should not discuss an ongoing investigation without counsel present.

[28] *Upjohn*, 449 U.S. at 394-95.

[29] *FTC v. GlaxoSmithKline*, 294 F.3d 141, 147 (D.C. Cir. 2002).

[30] *See United States v. Stein*, 463 F. Supp. 2d 459, 461-62 (S.D.N.Y. 2006).

[31] *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 758 (D.C. Cir. 2014) ("[C]ommunications made by and to non-attorneys serving as agents of attorneys in internal investigations are routinely protected by the attorney-client privilege."); *Voelker v. Deutsche Bank*, No. 11 Civ. 6362 (VEC), 2014 WL 4473351, at *1-2 (S.D.N.Y. Sept. 11, 2014).

Former employees. There is less consensus under U.S. law on whether communications with former employees are privileged. In the majority view, communications with former employees will be protected so long as they otherwise meet the *Upjohn* factors described above, and are once again given appropriate warnings as to the fact that counsel represents the company, not the employee.[32] Other courts, however, have held that such conversations are not privileged.[33] Thus, companies should give consideration to whether their respective jurisdictions allow for privilege in such circumstances or whether the other privileges discussed in this chapter would pertain to the relevant communications.

Third parties. Other than agents of counsel (as described above), the presence of a third party generally breaks the attorney-client privilege. However, there is an exception for third parties who are aiding the communication (e.g., a translator).[34]

Limitations of the attorney-client privilege in the corporate context

In general, the attorney-client privilege is construed narrowly.[35] Thus, it is important that companies keep in mind that certain categories of information are not protected by the attorney-client privilege.

Facts. The communication of facts *within* a privileged communication is protected. However, the privilege does not prevent compelled disclosure of the underlying facts.[36] Thus, "[t]he client cannot be compelled to answer the question, 'What did you say or write to the attorney?,' but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney."[37]

Business advice. The privilege *does not* extend to communications for the purposes of obtaining business, as opposed to legal, advice.[38] There are no "magic words" that

[32] *See, eg., In re Allen*, 106 F.3d 582, 605-06 (4th Cir. 1997); *U.S. ex rel. Hunt v. Merck-Medco Managed Care, LLC*, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004); *Peralta v. Cendant Corp.*, 190 F.R.D. 38, 40-41 (D. Conn. 1999).

[33] *See, eg., Infosystems, Inc. v. Ceridian Corp.*, 197 F.R.D. 303, 304-05 (E.D. Mich. 2000).

[34] *United States v. Ackert*, 169 F.3d 136, 139 (2d Cir. 1999).

[35] *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1126 (9th Cir. 2012) ("[W]e construe [the privilege] narrowly to serve its purposes" because it obstructs the "right to every man's evidence").

[36] *Upjohn*, 449 U.S. at 395.

[37] *Id*. at 396 (quoting *Philadelphia v. Westinghouse Electric Corp.*, 205 F. Supp. 830, 831 (E.D. Pa. 1962).

[38] *In re Cty. of Erie*, 473 F.3d 413, 419 (2d Cir. 2007).

make a communication one for legal purposes, as opposed to business purposes.[39] Instead, courts will look to "whether the communication was generated for the purpose of obtaining or providing legal advice as opposed to business advice."[40] Moreover, as discussed above, merely copying an attorney on a business communication or labeling a document "privileged" does not make it privileged.

Crime-Fraud Exception. Courts will apply a crime-fraud exception to pierce a privileged communication when "the client communication or attorney work product in question was *itself* in furtherance of the crime or fraud . . . and probable cause to believe that the particular communication with counsel or attorney work product was *intended* in some way to facilitate or to conceal the criminal activity."[41] If these elements are met, the attorney-client privilege will not protect any "client communications in furtherance of contemplated or ongoing criminal or fraudulent conduct."[42]

"Without prejudice" submissions to a regulator. U.S. courts have held that a broad settlement negotiation privilege, sometimes called a "without prejudice" privilege, is not necessary to achieve settlement. Therefore, U.S. courts do not recognize such a privilege, instead relying on Federal Rule of Evidence 408 (which prohibits certain uses of settlement offers against a party, as described below) to balance the policy favoring settlements against discovery rules.[43] The U.S. rule differs from many other jurisdictions, which recognize a "without prejudice" privilege that prevents compelled disclosure of communications with a regulator.[44] The specific contours of the "without prejudice" privilege differ among jurisdictions and are discussed later in this chapter.

Settlement discussions. In civil cases, conduct or statements made during compromise negotiations are not admissible to prove or disprove the validity or amount

---

[39] *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 758 (D.C. Cir. 2014).

[40] *In re Cty. of Erie*, 473 F.3d at 419.

[41] *In re Grand Jury Subpoenas Dated Mar. 2, 2015*, 628 F. App'x 13, 14 (2d Cir. 2015) (internal quotations omitted)(emphasis in original).

[42] *Id*.

[43] *In re MSTG Inc.*, 675 F.3d 1337, 1345 (Fed. Cir. 2012); *Matsushita Elec. Indus. Co. v. Mediatek, Inc.*, No. C-05-3148 (JCS), 2007 WL 963975, at *5 (N.D. Cal. Mar. 30, 2007) ("[W]hile there is a public policy of promoting settlement [of] disputes outside the judicial process, it [is] far from clear that a federal settlement privilege would result in increased likelihood of settlements so substantial that it would justify an exception to the production of evidence in support of the truth-finding process.").

[44] *E.g., Unilever Plc. v. The Proctor & Gamble Co.* [2000] 1 W.L.R. 2436 (Ir.); *Sable Offshore Energy Inc. v. Ameron Int'l Corp.* [2013] 2 S.C.R. 623 ¶ 19 (Can.) (quoting *Dos Santos Estate v. Sun Life Assurance Co. of Canada* (2005), 207 B.C.A.C. 54 ¶ 20 (Can.)).

of a disputed claim.[45] However, these statements are not protected from disclosure and are admissible for these purposes when offered in a criminal case or during negotiations with regulators.[46] Moreover, these statements can also be used to prove "a witness's bias or prejudice, negat[e] a contention of undue delay, or [to] prov[e] an effort to obstruct a criminal investigation or prosecution" in all criminal and civil contexts (including during negotiations with regulators).[47]

Self-incriminating statements. Clients can assert the Fifth Amendment privilege against self-incrimination in both criminal and civil contexts.[48] In criminal contexts, jurors are not permitted to use a defendant's refusal to testify to infer guilt or innocence.[49] However, in civil contexts, jurors may be permitted to infer guilt if a defendant invokes the privilege.[50] Corporations, in any event, cannot invoke the Fifth Amendment.[51]

Work Product Doctrine.

What is the work product doctrine?

The work product doctrine prevents compelled disclosure of materials created in the anticipation of litigation. The federal rule governing this doctrine states:

Ordinarily, a party may not discover documents and tangible items that are prepared, by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent), in anticipation of litigation or for trial.[52]

However, the work product doctrine provides only a qualified immunity from disclosure and, as with the attorney-client privilege, that immunity can be lost if not

[45] Fed. R. Evid. 408(a).

[46] Fed. R. Evid. 408(a)(2).

[47] Fed. R. Evid. 408(b).

[48] U.S. Const. amend. V; *Lefkowitz v. Turley*, 414 U. S. 70, 77 (1973) (citing *McCarthy v. Arndstein*, 266 U.S. 34, 40 (1924)) (holding that the Fifth Amendment "not only protects the individual against being involuntarily called as a witness against himself in a criminal prosecution but also privileges him not to answer official questions put to him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings.").

[49] *Griffin v. California*, 380 U.S. 609, 615 (1965).

[50] *Baxter v. Palmigiano*, 425 U.S. 308, 318 (1976) (holding "the Fifth Amendment does not forbid adverse inferences against parties to civil actions when they refuse to testify in response to probative evidence offered against them.").

[51] *See* Chapter III: Conducting an Internal Investigation, and Chapter VI: Employee Rights and Privileges.

[52] Fed. R. Civ. P. 26(b)(3).

carefully maintained. Courts differentiate between "opinion work product" and "fact work product." The former—which includes documents containing opinions and judgments of counsel on a matter, as opposed to bare facts or abstract discussions of legal theories—is virtually undiscoverable.[53] "Fact work product," by contrast, is discoverable if a party can "show[] that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."[54]

ELEMENTS:
THE WORK PRODUCT DOCTRINE

In determining whether to apply the privilege, courts look to:

— Whether materials were prepared "because of" the prospect of litigation, rather than in the ordinary course of business.

— Whether they represent opinion work product.

— If they do not, whether plaintiffs can establish a substantial need for the documents.[55]

Because the work product doctrine applies only to documents created in anticipation of litigation, it generally does not protect pre-existing records that were, or would have been, created in substantially similar form absent anticipated litigation.[56] Courts, however, do apply work product protections to the "selection and compilation" of particular documents, even where the documents themselves are not protected, because the selection process itself could reveal an attorney's opinions and mental impressions.[57] Courts have emphasized that this is a "narrow" exception, and the burden rests on the party asserting the work product privilege to persuade

[53] *See Holmgren v. State Farm Mut. Auto. Ins. Co.*, 976 F.2d 573, 577 (9th Cir. 1992); Fed. R. Civ. P. 26(b)(3) (a party cannot obtain "the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation").

[54] Fed. R. Civ. P. 26(b)(3).

[55] *See, e.g., Datel Holdings Ltd. v. Microsoft Corp.*, No. C-09-05535 (EDL), 2011 WL 866993, at *6-7 (N.D. Cal. Mar. 11, 2011); Fed. R. Civ. P. 26(b)(3).

[56] *In re Grand Jury Subpoenas Dated Mar. 19, 2002 and Aug. 2, 2002*, 318 F.3d 379, 384-85 (2d Cir. 2003).

[57] *Sporck v. Peil*, 759 F.2d 312, 316-17 (3d Cir. 1985).

the court that counsel's opinions will be revealed through the disclosure of the compilation of documents.[58]

Does the work product doctrine apply to governmental inquiries and internal investigations?

As discussed above, for the work-product doctrine to apply, material must have been prepared in anticipation of litigation. Moreover, the privilege will not shield documents created under "a generalized fear of litigation."[59] Thus, the question arises as to whether the work product doctrine applies to material prepared in response to a governmental investigation prior to, and which may or may not actually result in, litigation. In general, the threat of criminal or regulatory liability will sufficiently establish the threat of "litigation" required to bring a document within the work product doctrine.[60] Thus:

— An **internal investigation prompted by a government** subpoena or inquiry, or in anticipation of such subpoena or inquiry, gives rise to work product protection.[61]

— Even documents created as part of an **internal investigation initiated by the company** itself, without a regulatory inquiry, receives the same protections so long as the same threat of litigation is present. In other words, the person who created the documents "must at least have had a subjective belief that litigation was a real possibility, and that belief must have been objectively reasonable."[62]

[58] *Compare id*. at 316 (finding that documents selected to prepare a witness for deposition "could not help but reveal important aspects of [counsel's] understanding of the case"), *with In re Grand Jury Subpoenas*, 318 F.3d at 386-87 (finding that counsel had not shown with sufficient specificity that disclosure of selection of documents would reveal counsel's strategic thinking).

[59] *Lewis v. Wells Fargo & Co.*, 266 F.R.D. 433, 440-41 (N.D. Cal. 2010).

[60] *See Faloney v. Wachovia Bank, N.A.*, 254 F.R.D. 204, 214-16 (E.D. Pa. 2008); *see also Martin v. Bally's Park Place Hotel & Casino*, 983 F.2d 1252, 1261 (3d Cir. 1993).

[61] *See United States v. ISS Marine Servs., Inc.*, 905 F. Supp. 2d 121, 136-37 (D.D.C. 2012).

[62] *In re Sealed Case*, 146 F.3d 881, 884 (D.C. Cir. 1998).

PRACTICE TIP: PREPARING A DOCUMENT IN ANTICIPATION OF LITIGATION

A document is prepared in anticipation of litigation if "it can fairly be said that the 'document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation[.]'"[63] Litigation does not need to be the primary or only motive behind the document's creation. For example, the document can also be used for ordinary business purposes such as assisting in making a business decision influenced by the likely outcome of a potential litigation.[64] In order to better ensure a finding of privilege, however, the document should be labeled as attorney work product, and the involvement of the litigator who is anticipating litigation should be noted in the timekeeping files.[65]

CASE STUDY: WHEN AN INTERNAL AUDIT IS NOT PROTECTED

In the *ISS Marine* case, the court grappled with a scenario in which "the person preparing [an] [a]udit [r]eport was both acting as an investigator into a specific allegation of wrongdoing and was also arguably trying to protect the company from the possibility of future litigation."[66] The court, in finding that the work product privilege did not apply, reasoned that the company "would have conducted this internal investigation 'in the ordinary course of business' irrespective of the prospect of litigation" and, therefore, the work product doctrine did not apply. The court came to this conclusion, in part, because the investigation that lead to the audit report "was conducted by a non-attorney who never communicated with outside counsel."[67]

[63] *In re Grand Jury Subpoena (Mark Torf/ Torf Envtl. Mgmt.)*, 357 F.3d 900, 908 (9th Cir. 2004) (alteration in original) (quoting *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998)).

[64] *Id.*; *United States v. Deloitte LLP*, 610 F.3d 129, 138 (D.C. Cir. 2010); *see also Adlman*, 134 F.3d at 1198.

[65] *Cf. Local 851 of Int'l Bhd. of Teamsters v. Kuehne & Nagel Air Freight, Inc.*, 36 F. Supp. 2d 127, 132 (E.D.N.Y. 1998) (noting that waiver of attorney-client privilege had occurred because counsel "did not take reasonable precautions to avoid disclosure," including "[m]ost notably, defendants' counsel failed to label the Letter as confidential").

[66] *United States v. ISS Marine Servs., Inc.*, 905 F. Supp. 2d 121, 136 (D.D.C. 2012).

[67] *Id.* at 137-38.

Other Privilege Doctrines

Common interest privilege

One important exception to the rule that sharing a privileged document with a third party results in a waiver of the privilege is the "common interest privilege" doctrine. Under this doctrine, the act of sharing an otherwise privileged communication with counsel for another party on a matter of common legal interest does not result in a waiver of the privilege if the parties agree for those communications to be kept confidential and they share a common interest. For example, if one (or many) plaintiff(s) is suing multiple defendants for similar actions based on the same core events, and the defendants want to pursue a similar, joint defense, they may seek to enter into a common interest agreement. The "common interest" must be a *legal* interest, not a *business* or commercial interest.[68] The legal interest does not need to involve actual litigation.[69]

ELEMENTS:
THE COMMON INTEREST PRIVILEGE

- The underlying communication must itself be privileged.
- The parties share a common interest.
- The disclosing party had a reasonable expectation of confidentiality.
- The "disclosure. . .must be reasonably necessary for the accomplishment of the purpose for which the lawyer was consulted."[70]

While there must be a "common interest" for the doctrine to apply, parties' interests do not have to be aligned on every issue in order for the common interest privilege to apply so long as the exchange of information is with regard to the matter the parties do have in common.[71] Further, the fact that clients with common interests

[68] *Pampered Chef v. Alexanian*, 737 F. Supp. 2d 958, 964-65 (N.D. Ill. 2010).

[69] *United States v. United Techs. Corp.*, 979 F. Supp. 108, 112 (D. Conn. 1997) (exchanges among five aerospace companies that formed a consortium to break General Electric's dominance in the small-engine market and shared interest in minimizing tax liability).

[70] *OXY Res. Cal. LLC v. Superior Court*, 115 Cal. App. 4th 874, 891 (Cal. Ct. App. 2004) *modified* Mar. 4, 2004; Restatement (Third) of the Law Governing Lawyers § 76 (2000).

[71] Restatement (Third) of the Law Governing Lawyers § 76 (2000).

also have interests that conflict—perhaps sharply—does not necessarily mean that communications on matters of common interest are non-privileged.[72]

In order to help ensure a court will respect the common interest privilege, a company should consider whether to enter into a written common interest agreement. The decision whether to document the common interest agreement in writing is frequently a complicated one that requires consideration of a number of different issues. However, while a written agreement is not mandatory in order to maintain the common interest privilege, a common interest agreement can:

— Define the scope of the interest.

— Evidence that the parties share a common interest.

— Evidence the company's reasonable expectation of confidentiality.

— Specify how the agreement is to end and what happens with the privileged communications once the agreement ends.

— Document that the existence of the common interest agreement does not create an attorney-client relationship among all the parties to the agreement.

[72] *Eisenberg v. Gagnon*, 766 F.2d 770, 787-88 (3d Cir. 1985).

PRACTICE TIP:
MAINTAINING THE COMMON INTEREST PRIVILEGE

- Ensure all parties operate under a reasonable expectation of confidentiality through an explicit understanding among all parties that the communications are confidential.
- Delineate the scope of the privilege at the outset.
- Mark communications as confidential and subject to common interest privilege.
- Though not required, consider whether to memorialize the common understanding in an written agreement.
- Keep records that indicate the sharing of ideas about the matter is "reasonably necessary for the accomplishment of the purpose for which the attorney disclosing was consulted."[73]

Self-critical analysis privilege

Some courts have recognized a possible privilege relevant to audits or internal investigations, a so-called self-critical analysis privilege.[74] In order to obtain the benefit of this privilege, "[i] the information must result from a critical self-analysis undertaken by the party seeking protection; [ii] the public must have a strong interest in preserving the free flow of the type of information sought; [iii] the information must be of the type whose flow would be curtailed if discovery were allowed."[75] This privilege, however, is not recognized in every jurisdiction.[76]

The bank examination privilege

The bank examination privilege is largely codified in 12 U.S.C. § 1828(x). This privilege belongs to a bank regulator, such as the Consumer Financial Protection Bureau ("CFPB"), Office of the Comptroller of the Currency ("OCC"), Federal Reserve Bank ("Fed"), and the Federal Deposit Insurance Corporation ("FDIC"). When invoked, the regulator may refuse to produce information a company has

[73] *Meza v. H. Muehlstein & Co.*, 176 Cal. App. 4th 969, 981 (Cal. Ct. App. 2009); Restatement (Third) of the Law Governing Lawyers § 76 (2000); *Cooey v. Strickland*, 269 F.R.D. 643, 652 (S.D. Ohio 2010); *Hanover Ins. Co. v. Rapo & Jepsen Ins. Servs., Inc.*, 870 N.E.2d 1105, 1113 (Mass. 2007).

[74] *See, e.g., Bredice v. Doctors Hosp. Inc.*, 50 F.R.D. 249, 251 (D.D.C. 1970).

[75] *Dowling v. Am. Haw. Cruises, Inc.*, 971 F.2d 423, 426 (9th Cir. 1992).

[76] *See, e.g., Ovesen v. Mitsubishi Heavy Indus. of Am. Inc.*, No. 04 Civ. 2849(JGK)(FM), 2009 WL 195853, at *2 (S.D.N.Y. Jan. 23, 2009) (collecting cases) ("Although some federal courts have recognized a self-critical analysis privilege, its continuing viability is an open question.").

given it in the course of a supervisory or regulatory process.[77] Because this privilege belongs to the regulator, only the regulator can waive privilege.

Waiver of Privileges

Companies must scrupulously protect against disclosure of their privileged materials in order to avoid inadvertently waiving applicable privileges and permitting compelled disclosure to others.

Accidental disclosure

Companies must guard against accidental disclosure of privileged materials. Although accidental disclosure can sometimes lead to waiver, particularly if the company has not taken (and documented) sufficient steps to guard against inadvertent disclosure, companies can take steps to prevent this harsh outcome. The Federal Rules of Evidence also protect truly inadvertent disclosures of otherwise privileged materials to government agencies. Pursuant to FRE 502(b), an inadvertent disclosure of information "in a federal proceeding or to a federal office or agency" will not operate as a waiver where:

— The disclosure was inadvertent.

— The holder of the privilege took reasonable steps to prevent disclosure.

— The holder promptly took steps to rectify the error.[78]

However, any accidental disclosure presents a risk that a court will find waiver, and companies should, therefore, institute procedures to ensure that inadvertent production is either avoided altogether or minimized by prompt discovery and correction of inadvertently produced documents. One of the most effective ways of doing this is entering into a "claw-back" agreement with the other party, which allows either party to claw back—i.e., demand the return of—documents that have been inadvertently disclosed. The parties should include, as part of the agreement,

[77] 12 U.S.C. § 1828(x) (2018).

[78] *See Bayliss v. N.J. State Police*, 622 F. App'x 182, 186 (3d Cir. 2015).

an explicit statement that inadvertent disclosure is not a waiver. In addition, if a document has been inadvertently disclosed, the company should take immediate steps to retrieve it and should document those steps—in part to demonstrate that it is zealously guarding the privilege.

PRACTICE TIP:
AVOIDING WAIVER OF INADVERTENTLY DISCLOSED INFORMATION

Although the procedures set out in FRE 502(b) provide a mechanism for attempting to prevent an inadvertent disclosure from becoming a waiver, the best way to ensure no waiver is to prevent the inadvertent disclosure. Companies should, therefore:

- Establish good document review protocols in advance of producing documents.
- Mark relevant documents as "Privileged and Confidential."
- Enter into a claw-back agreement.
- Establish a procedure to seek the immediate return of documents that were inadvertently produced.

Purposeful disclosure

There are circumstances under which a company may wish to voluntarily disclose otherwise privileged information to a government authority during the course of an investigation. A company may choose to make such disclosures, for example: (i) to assert an advice of counsel defense;[79] (ii) to provide the government with exculpatory facts; or (iii) to obtain credit for cooperating with the government's investigation.[80] However, companies should understand the risks associated with voluntary disclosure of otherwise privileged materials.

U.S. courts generally do not recognize a party's ability to selectively waive privilege. In most instances, "a party cannot partially disclose privileged communications or affirmatively rely on privileged communications to support its claim or defense

[79] The defense of advice of counsel can be used to defeat an element of a claim (*e.g.*, intent) or establish an element of a defense (*e.g.*, good faith) based on reliance on counsel's advice of the legality of the underlying conduct. *See, e.g., United States v. Bilzerian*, 926 F.2d 1285, 1292 (2d Cir. 1991). However, to assert it, the company must waive privilege and disclose the underlying advice. *Id.*; *In re Cty. of Erie*, 546 F.3d 222, 228 (2d Cir. 2008).

[80] *See* Chapter VII: Public Relations & Message Management.

and then shield the underlying communications from scrutiny by the opposing party."[81] Companies seeking to disclose part of a privileged communication for advantageous purposes should, therefore, beware that a court may well require the disclosure of the entire communication, or of other privileged communications relevant to understanding the legal advice sought or received not only with respect to the immediate governmental inquiry, but for all purposes later on, including any follow-on civil litigation.

PRACTICE TIP: CONFIDENTIALITY AGREEMENTS WITH GOVERNMENTAL AUTHORITIES—ARE THEY WORTHWHILE?

Companies may decide to enter into confidentiality agreements with government authorities in advance of producing possibly-privileged materials seeking to maintain privilege by making it clear that the company's production of any privileged documents to the government is not intended as a general waiver of privilege over those, or other, documents.

Confidentiality agreements are hardly a perfect solution, however. Not only does the weight of federal case law suggests that such agreements not only fail to automatically protect privilege in follow-on civil litigation, but courts also frequently require the production to private parties of the materials produced to the government even where a confidentiality agreement was in place.[82]

However, entering into a confidentiality agreement is most likely a worthwhile endeavor nonetheless because a company may later be able to argue that its waiver was, at most, limited to those documents it actually produced to the government, as opposed to a broader waiver of all privileged materials concerning the relevant subject matter.[83]

[81] *In re Grand Jury Proceedings*, 219 F.3d 175, 182–83 (2d Cir. 2000). Only the Eighth Circuit has embraced the "selective disclosure" theory, under which a litigant can disclose materials to the government but not waive the privilege as to civil litigants. *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (en banc). Every other circuit to consider this issue has rejected the Eighth Circuit's theory. *See, e.g., In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127 (9th Cir. 2012) (collecting cases).

[82] *In re Pac. Pictures Corp.*, 679 F.3d at 1128-29; *but see In re Steinhardt Partners, L.P.*, 9 F.3d 230, 236 (2d Cir. 1993) (suggesting in dicta that confidentiality agreement with SEC may preserve work-product privilege).

[83] *See In re Mut. Funds Inv. Litig.*, 251 F.R.D. 185, 188 (D. Md. 2008) (waiver limited to material actually disclosed).

Steps to preserve privilege during government investigations

There are a number of practical steps that companies should consider in order to avoid waiving any legal privileges they may otherwise be entitled to assert in a U.S. investigation or in a related legal proceeding.

PRACTICE TIP:
CHECKLIST FOR PRESERVING PRIVILEGE DURING GOVERNMENT INVESTIGATIONS

- Get attorneys involved early.
- Limit distribution of materials to those who "need to know."
- Set out clear areas of responsibility.
- Mark documents as "confidential" and "privileged" when they are distributed, so they can easily be identified during productions.
- Thoroughly review documents for privilege before producing to the government.
- Give appropriate *Upjohn* warnings informing the interviewee of the company position that privilege applies and that the interview should be kept confidential, before employee interviews.
- Observe appropriate note-taking practices during interviews.
- Make it clear early and often that you are not waiving your privileges.
- Enter into a confidentiality and claw-back agreement with governmental authorities.

Getting started

Responding to large-scale requests from regulators requires organization. Clear reporting lines and areas of responsibility can go a long way toward minimizing the risks that (i) documents are inadvertently produced, or (ii) information is not treated in a way necessary to maintain confidentiality.

Involve counsel early

It is important to involve attorneys early because an investigation undertaken solely by management may not be subject to privilege protections.[84] If a company is to maintain that a document is created in anticipation of litigation, it is useful that a litigator be involved in the creation of the document.

Consider applicable law

Particularly in cross-border investigations, the substantive privilege law of the multiple jurisdictions involved in the investigation may differ. Companies should take stock of the relevant law that could apply, and also consider how a court may resolve a choice-of-law analysis if presented with a privilege dispute.[85]

Involving Employees and Officers

In addition, it is important from the outset to think about who should be involved in the investigation. Because maintaining the confidentiality of advice received is critical to maintaining the privilege, companies conducting an investigation or responding to government inquiries should keep people involved on a "need to know" basis and, generally, should keep the circle of those involved with, or who have knowledge of, the investigation as small as possible. Thus, only include those whose duties require them to be involved and senior level officers. In addition, impress upon all employees involved, both current and former, the need to maintain confidentiality, and ensure that those involved know what role they are to play in the investigation and how to avoid divulging privileged materials. Note that, if former employees must be involved, communications between them and counsel may not be privileged, so consider arranging for individual counsel for those individuals and entering into a common interest privilege agreement.

---

[84] *In re Grand Jury Subpoena*, 599 F.2d 504, 510 (2d Cir. 1979) ("To the extent that an internal corporate investigation is made by management itself, there is no attorney-client privilege.").

[85] *See, e.g., Astra Aktiebolag v. ANDRX Pharms., Inc.*, 208 F.R.D. 92, 98 (S.D.N.Y. 2002); *In re Rivastigmine Patent Litig.*, 237 F.R.D. 69, 76 (S.D.N.Y. 2006) (rejecting privilege claims under Swiss law, which, unlike U.S. law, does not create privilege for communications with in-house counsel), *aff'd in relevant part*, 239 F.R.D. 351, 356-59 (S.D.N.Y. 2006); *Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 69-70 (S.D.N.Y. 2010).

Dealing with documents

Maintain confidentiality.

Mark every page of a privileged document "Privileged & Confidential." Failure to mark documents as privileged may make it more difficult to make a privilege claim later on.[86] Note, however, that simply marking a document as "Confidential" or "Privileged" does not in and of itself protect a document from disclosure if it is not subject to an otherwise valid privilege assertion.[87] But failure to mark a page as privileged and confidential can result in a waiver if that page is lost or misplaced and ends up in the hands of a third party.[88]

Prepare privilege logs.

In the United States, a company facing a governmental inquiry may well be required to articulate any claimed privilege and to describe the nature of any withheld documents in a way that will enable the agency or other relevant parties to assess the claim.[89] Thus, when withholding documents in a discovery request (from the government or otherwise), companies should create privilege logs. These logs should list the withheld documents and carefully document the rationale for withholding production on the basis of privilege.

Make a FOIA Confidentiality Request.

The Freedom of Information Act ("FOIA") generally gives the public the ability to access information in the federal government's possession. When producing documents or other information to a governmental agency, companies should request confidential treatment under FOIA in order to avoid disclosure. To do so, the company should submit a letter requesting confidential treatment of the materials

[86] *See, e.g., J.N. v. S. W. Sch. Dist.*, 55 F. Supp. 3d 589, 600 (M.D. Pa. 2014) ("The email in question does not bear indicia of those precautions, such as a 'privileged' or 'confidential' label.").

[87] *See In re Google Inc.*, 462 F. App'x 975, 979 (Fed. Cir. 2012) (email marked "confidential" not privileged "in light of the remainder of the email").

[88] Note, however, that if an adversary receives a document that is plainly privileged, the adversary is required to promptly return the inadvertently disclosed document. *See, e.g., Stinson v. City of New York*, No. 10 CIV. 4228 RWS, 2014 WL 5090031, at *4 (S.D.N.Y. Oct. 10, 2014) ("[T]he Association of the Bar of the City of New York has found that while lawyers are ethically bound to return or destroy inadvertently disclosed documents, the non-disclosing lawyer is not ethically barred from using information gleaned prior to knowing or having reason to know that the communication contains information not intended for the non-disclosing lawyer."); *see also* Model Rules of Prof'l Conduct r. 4.4(b) (Am. Bar Ass'n 2018). ("A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.").

[89] This is a requirement of the Federal Rules of Civil Procedure and of many administrative agency subpoenas. *See, e.g.*, Sec. Exch. Comm'n, Enforcement Manual § 3.2.7.4 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. (directing Division of Enforcement staff to obtain privilege logs during investigations).

pursuant to the applicable law, as well as ensuring that any such requests comply with the regulations and practices of the relevant agencies.[90]

PRACTICE TIP:
CONDUCTING INTERVIEWS

- Limit attendance to attorneys, note takers, or agents or investigators of attorneys acting at their direction.
- Assign a single note taker.
- Consider addressing any notes taken to a client as an attorney-client communication.
- Administer the *Upjohn* warnings at the beginning of each interview, confirm that the witness understands the warning, and offer to answer any questions.
- Ensure that the administration of the *Upjohn* warning and the witness's understanding of that warning are memorialized in the interview memorandum.
- Where the memorandum includes both facts and mental impressions that should be made clear on the face of the memorandum.

Interviews

In addition to collecting documents, interviewing employees is an important part of any internal investigation. However, as discussed above, companies must ensure that such interviews do not result in a privilege waiver. Employee interviews should be undertaken by an attorney or an agent of an attorney acting at the attorney's direction in order to ensure that what is said in the interview remains privileged. This practice extends to notetaking during interviews. Moreover, purely factual recitations of an interview—set out, for example, in an interview memorandum—are accorded lesser protection under the work product doctrine than opinion work product. Thus, standard practice is for an attorney's notes to be memorialized in a formal memorandum that, in addition to describing the facts as the witnesses perceived them, sets out the attorney's mental impressions and opinions of the interview. In addition, it is good idea to have a single note taker, who will then turn those notes

[90] *See, e.g.*, 17 C.F.R. § 200.83 (2018) (Securities and Exchange Commission); 17 C.F.R. § 145.9 (2018) (Commodity Futures Trading Commission).

into an interview memorandum that includes mental impressions, legal theories, and advice. This serves both: (i) to avoid having conflicting notes in the event that the attorneys' notes are ever required to be produced to a regulator or in litigation; and (ii) to make it easier to convert the notes into an interview memorandum setting out the attorney's mental impressions of the interview. In addition, it is frequently helpful to set out a protocol regarding whether handwritten notes of an interview will be reduced to a written memorandum and what to do with the notes after the written memorandum is completed and to follow that protocol consistently.

PRACTICE TIP:
COMMUNICATING WITH GOVERNMENT AGENCIES

When dealing with the government, the company should endeavor to:

- Affirmatively note, in writing if possible, that it does not intend to waive privilege.
- Avail itself of all statutory protections from waiver of privilege.
- Consider entering into a confidentiality agreement with the regulator.
- Consider entering into a claw-back agreement with the regulator.
- Seek immediate claw-back in the event of an inadvertent production.
- If considering a waiver, define an agreed-upon scope with the regulator in writing.
- Consider providing summaries in oral—not written—presentations in order to prevent other parties from obtaining the written summary provided to the regulator and limit disclosures and presentations to factual material.
- When addressing partially privileged documents, consider redaction vs. withholding.
- Send a FOIA confidentiality request to the regulator, which may shield the communications from FOIA requests.

Communicating with the Regulator

When communicating with a relevant authority, companies should take care to make it clear that they do not intend to waive privilege in communications unless—and until—they choose to do so. Thus, in addition to the above, there are a number of steps that companies can take to best protect their privileges in communications with regulators.

England and Wales[91]

Summary

Key Privileges:

— ***Legal Advice Privilege:*** Protects the substance of confidential lawyer-client communications made for the purposes of the giving or obtaining of legal advice.

— ***Litigation Privilege:*** Protects the substance of confidential documents created where litigation is in reasonable contemplation and where the documents are for the dominant purpose of such litigation.

— ***Working Papers Privilege:*** Protects documents which, if disclosed, would betray the trend of the legal advice being given by a lawyer.

Key Practice Points:

— In English proceedings, English privilege law will be applied to determine whether a document is privileged. Documents which are not privileged under English law, but which may be privileged under a foreign law, will likely be subject to disclosure in English proceedings.

— All lawyer-client communications should be marked "Privileged and Confidential." This label does not create privilege (and its absence will not, by itself, cause a loss of privilege), but will help to subsequently identify and evidence privileged material.

— Generally, advice provided by an in-house lawyer may enjoy a privilege under English law. However, communications with in-house legal counsel in the context of a European Commission investigation will usually not be privileged. In these circumstances, in order to preserve privilege, external counsel should be retained.

[91] For ease of reference, the English and Welsh jurisdiction is referred to in this section as "English" jurisdiction.

— Only those individuals who have been given responsibility for coordinating the organization's communications with its lawyers will be considered part of the "client" for the purposes of legal advice privilege. Therefore, communications between lawyers and employees who are not responsible for coordinating the organization's communications with legal advisers (irrespective of their seniority) will not be privileged.

— Where there is a current or prospective English nexus to a dispute or investigation, organizations should seek to identify, and record in writing, those individuals who will form part of the "client" group. To avoid uncertainty as to the position of in-house lawyers, where possible, in-house lawyers should not be included within the "client" group designated to be responsible for coordinating the organization's communications with lawyers.

— In the absence of adversarial litigation, records of internal investigation interviews will not be privileged unless the interviewee is within the "client" group.

— Documents recording communications between lawyers and individuals outside the "client" group will only be privileged where they are created for the dominant purpose of adversarial litigation. It is not sufficient that the relevant litigation is one of multiple purposes for which a document is created.

— It should be assumed that regulatory or criminal investigations where the investigating authority has not made formal allegations may not constitute adversarial litigation and that, in that circumstance, litigation privilege will not apply.

— Where adversarial litigation is in reasonable prospect, the organization should contemporaneously record that fact (whether in board minutes or otherwise). Equally, where a document has been prepared for the dominant purpose of adversarial litigation, this should be recorded in the body of the document. These statements will not create privilege (and their absence will not, by itself, cause a loss of privilege), but will help identify and evidence privileged material.

— In some circumstances, a limited waiver of privilege is recognized under English law, where privileged material is confidentially disclosed to a third party for specified purposes on the express or implied terms that privilege is not waived in the material.

Key Differences Between English and U.S. Privileges

While English privilege law shares many characteristics with its U.S. counterpart, there are certain distinguishing characteristics of English legal privilege law that may not instinctively be familiar to practitioners in other jurisdictions.

PRACTICE TIP:

English Privilege	U.S. Privilege
— Narrow conception of the "client" which usually will not encompass all employees within an organization.	— The "client" group will generally encompass all employees within an organization.
— Where adversarial litigation is not in reasonable prospect, communications with third parties are usually not covered by privilege.	— Privilege can apply to communications with third parties where the purpose is to assist the lawyer in providing legal advice.
— A recognized concept of a limited waiver of privilege.	— Limited waiver of privilege not recognized in many jurisdictions.
— Criminal and regulatory investigations are generally not considered "adversarial" until allegations or charges are formally levied.	— Criminal or regulatory investigations generally engage privilege.

Choice of Law

The English courts apply the *lex fori* to determine whether a communication is privileged.[92] As a result, in proceedings in the English courts, English law will be applied to determine privilege issues.[93]

Although in English civil proceedings, the court retains discretion to allow a party to resist disclosing a document (which is not otherwise protected from disclosure on privilege or other grounds) where disclosure would damage the public interest,[94] the fact that a document is privileged under a foreign law is unlikely in and of itself to result in the court exercising that discretion, particularly where there is a current or prospective English nexus to a dispute.[95]

Legal Advice Privilege

ELEMENTS: LEGAL ADVICE PRIVILEGE

To be covered by legal advice privilege, communications must be:

— Confidential.

— Made between a lawyer and a client.

— Made for the purposes of giving or receiving legal advice.

Lawyer-Client Communications

As a general matter, all lawyer-client communications should be marked "Privileged and Confidential." This label does not create privilege, but will help to subsequently identify privileged material and can be useful in preserving privilege in the event of an inadvertent disclosure.

[92] Thanki, "The Law of Privilege" (2d ed.) at 4.84, as affirmed in The RBS Rights Issue Litigation [2016] EWHC 3161 (Ch)

[93] *Lawrence v Campbell* [1859] 4 Drew 485.

[94] Civil Procedure Rules, 31.19(1).

[95] *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

Lawyers

A "lawyer" means a qualified solicitor or barrister.[96] Communications with overseas lawye rs may also be privileged.[97]

Save in the case of investigations by the European Commission (where external counsel should be retained and instructed),[98] legal advice privilege may also attach to communications involving qualified in-house lawyers. Communications between parties and non-legally qualified personnel (e.g. clerks, trainees, secretaries, or paralegals) will likewise attract privilege provided that, at the time of the communication, the individual is acting under the supervision of a qualified lawyer.[99]

Clients

English law adopts a narrow definition of what constitutes a "client" for the purposes of legal advice privilege.

Three Rivers 5 remains the governing authority on the formulation of the "client" for the purposes of legal advice privilege.[100] Its effect is that only those individuals who have been given responsibility for coordinating the organization's communications with its lawyers will be considered part of the "client" for the purposes of legal advice privilege, and communications between lawyers and those employees outside this group (irrespective of their seniority) will not be privileged.

The decision has caused significant difficulties for organizations in the context of internal investigations, including through narrow interpretations of what constitutes the "client group."

---

[96] *R (on the application of Prudential plc and another) v. Special Commissioner of Income Tax and another* [2013] UKSC 1.

[97] Bankim Thanki, *The Law of Privilege* (3rd Ed. 2018) at 2.37.

[98] *In Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. Commission* (Case C-550/07 P), the Court of the Justice of the European Union held that legal professional privilege does not apply to communications between a company and its in-house lawyers in the context of EU antitrust investigations.

[99] *Taylor v. Forster* (1825) 2 C&P 195; *Wheeler v. Le Marchant* (1881) 17 Ch D 675.

[100] The principle was affirmed in *The RBS Rights Issue Litig.* [2016] EWHC 3161 (Ch) and *Serious Fraud Office v. Eurasian Nat. Resources Corp. Ltd.* [2017] EWHC 1017 (QB).

CASE STUDY:
THREE RIVERS COUNCIL V. BANK OF ENGLAND ("THREE RIVERS 5")[101]
WHO IS THE "CLIENT"?

Following the collapse of Bank of Credit and Commerce International ("BCCI") in 1991, an inquiry was established to investigate the supervision of BCCI and to review the actions taken by the U.K. government. The so-called "Bingham Inquiry" published its report in 1992, and the liquidators of BCCI subsequently issued proceedings against the Bank of England ("BoE") for losses caused by the collapse.

The plaintiffs sought from the BoE documents prepared by BoE employees which were provided to its external counsel for the purposes of preparing the BoE's submissions to the Bingham Inquiry. The BoE claimed that these documents were covered by legal advice privilege.

The English Court of Appeal held that, for the purposes of assessing legal advice privilege, the "client" did *not* encompass all employees of the BoE, but was confined to a particular group of individuals (the "Bingham Inquiry Unit" or BIU) who had been given responsibility for coordinating the BoE's communications with the BoE's lawyers. Any employees not forming part of the BIU (including even, hypothetically, the Governor of the BoE himself) were considered to be third parties, whose communications would *not* themselves be covered by legal advice privilege.

Where there is a current or prospective English nexus to a dispute or investigation, organizations should seek to identify, and record in writing, those individuals who will form part of the "client" group. To avoid uncertainty as to the position of in-house lawyers, where possible, in-house lawyers should not be included within the "client" group.[102]

[101] *Three Rivers DC v. Bank of England* [2003] EWCA Civ. 474.

[102] *See also* § 3(b): Giving or Obtaining Legal Advice.

CASE STUDY:
THE RBS RIGHTS ISSUE LITIGATION[103]
LEGAL ADVICE PRIVILEGE IN INTERNAL INVESTIGATIONS

The defendant's shareholders sought to recover investment losses on the basis that the defendant's prospectus for a 2008 rights issue was inaccurate and incomplete. The shareholders sought disclosure of notes from interviews conducted by the defendant's lawyers with current and former employees during two internal investigations. The defendant resisted the application, amongst other grounds, because the interview notes were covered by legal advice privilege, given that the interviewees were authorized to communicate in confidence with the defendant's lawyers.

The English High Court rejected this argument, holding that, based on *Three Rivers 5*, the employee interviewees did not form part of the "client" group for the purposes of legal advice privilege, and therefore the interviews (and the notes recording them) were not privileged. The fact that the notes were not disputed to be privileged under U.S. law did not change this analysis.

Communications

In addition to communications between a lawyer and client, legal advice privilege may cover drafts of such communications.[104] In addition, in some circumstances, privilege may be retained where records of privileged legal advice are confidentially disseminated throughout an organization[105] or outside an organization,[106] although the permissible limits of such communications are difficult to define. For prudence, outside the context of adversarial litigation (as to which, see discussion below), it should generally be assumed that communications between an organization's lawyers and individuals outside the "client" group, or material that is disseminated to employees outside of the "client" group, will not be privileged. Organizations should therefore strictly limit the circulation of privileged information with employees outside the "client" group to where it is strictly necessary, and should do so expressly pursuant to a limited waiver of privilege (also discussed below).

[103] The RBS Rights Issue Litigation [2016] EWHC 3161 (Ch).

[104] *Three Rivers DC v. Bank of England* [2003] EWCA Civ 474.

[105] *Bank of Nova Scotia v. Hellenic Mut. War Risks Assoc. (Bermuda) Ltd. (The "Good Luck")* [1992] 2 Lloyd's Rep 540.

[106] *USP Strategies Plc v. London Gen. Holdings Ltd.* [2004] EWHC 373 (Ch).

Giving or Obtaining Legal Advice

Legal advice includes "advice as to what should prudently and sensibly be done in the relevant legal context."[107] To determine whether the advice was given in the "relevant legal context," the court will consider whether the advice sought or received relates to the "rights, liabilities, obligations or remedies" of the client under private or public law.[108]

Although the English courts have generally interpreted the "relevant legal context" test widely, difficulties can arise where advice is given to an organization by their in-house lawyer where that lawyer also holds another position within the organization. In such circumstances, English Courts will decide whether the individual was giving advice in their capacity as a lawyer or in some other business capacity.[109] To avoid uncertainties, in matters where a lawyer may be asked to give both business and legal advice, that lawyer should, where possible, not provide legal advice to the organization.

Litigation Privilege

ELEMENTS: LITIGATION PRIVILEGE

To be covered by litigation privilege, communications must be:

— Confidential.

— Made at a time when adversarial litigation was in reasonable prospect.

— Made for the dominant purpose of such proceedings.

[107] *Balabel v. Air India* [1988] 1 Ch 317.

[108] *Three Rivers DC and others v. Governor and Co. of the Bank of Eng.* [2004] UKHL 48.

[109] *Blackpool Corp. v. Locker* [1948] 1 KB 349.

Adversarial Litigation

Whether or not proceedings are sufficiently "adversarial" will depend on the circumstances. Litigation or arbitral proceedings (whether domestic or overseas) will be sufficiently adversarial to attract litigation privilege.[110]

The status of regulatory or criminal investigations is uncertain and will depend on the facts. In *Tesco Stores Limited v Office of Fair Trading*,[111] the Competition Appeal Tribunal held that notes of third-party witness interviews conducted by a company's lawyers were subject to litigation privilege as, by the time the interviews took place, the Office of Fair Trading had issued two Statements of Objection formally alleging breaches of U.K. competition legislation, and proceedings were therefore "sufficiently adversarial" to engage litigation privilege. Although the case arose in the context of a U.K. competition investigation, it is prudent to assume that the principle that an investigation by a U.K. public authority does not become "adversarial" unless and until the authority communicates formal allegations against the entity under investigation will apply generally to regulatory or criminal investigations. For instance, the High Court in *Serious Fraud Office v ENRC*[112] held that, on the facts, the criminal investigation by the Serious Fraud Office into the defendant company was not adversarial litigation for these purposes.

Reasonable Prospect

For litigation privilege to apply, adversarial litigation must be in reasonable prospect. The English Court of Appeal has opined that "a general apprehension of future litigation" or "a distinct possibility that sooner or later someone might make a claim" were not sufficient to engage litigation privilege.[113]

[110] Bankim Thanki, The Law of Privilege (3rd Ed. 2018) at 3.61 – 3.63.

[111] *Tesco Stores Ltd. v. Office of Fair Trading* [2012] CAT 6.

[112] *Serious Fraud Office (SFO) v. Eurasian Nat. Resources Corp. Ltd.* [2017] EWHC 1017 (QB).

[113] *United States of America v. Philip Morris Inc. and others* [2004] EWCA Civ 330.

The English case law on when litigation is in "reasonable prospect" is not easy to reconcile, and contradictory principles can be observed. Where adversarial litigation involving the organization is in reasonable prospect (for instance, because proceedings involving the organization have been threatened), this should be contemporaneously recorded (for instance, through a legal opinion or in committee or board minutes). This will not guarantee that litigation privilege will cover communications with third parties created for the dominant purpose of that litigation will be privileged, but will help to establish the organization's state of mind at the time of the creation of the document.

Dominant Purpose

Notwithstanding that adversarial litigation was in reasonable prospect at the time of a communication, litigation privilege will not apply unless the communication was made for the "dominant purpose" of that litigation. In the regulatory/criminal investigations context, the English High Court has held that documents created for the purpose of *avoiding* an investigation are not created for the dominant purpose of adversarial litigation.

CASE STUDY:
SERIOUS FRAUD OFFICE V. ENRC[114]

The English High Court held that the principal purpose of documents created during an internal investigation was to establish the accuracy of allegations made by a whistleblower, and to decide on any consequential action. In addition, the court opined that, even if the sole purpose of the preparation of the documents in question was for contemplated criminal proceedings, "avoidance of a criminal investigation cannot be equated with the conduct of a defense to a criminal prosecution."

The ENRC decision is subject to an appeal which was heard in July 2018. Judgment is awaited.

[114] *Serious Fraud Office (SFO) v. Eurasian Nat. Resources Corp. Ltd.* [2017] EWHC 1017 (QB).

As with the case law on whether litigation is in reasonable prospect, it is difficult to reconcile the contrasting approaches taken to date in the case law on "dominant purpose."[115] For example, courts have found, in some cases, a number of equally prominent but distinct "dual purposes" to a communication, with the result that litigation privilege will not apply to those communications.[116] On the other hand, however, courts have likewise been prepared to find that dual purposes were, in reality, components of a single, overarching purpose relating to the litigation.[117] Where a communication between a lawyer, or a member of the client group, and a third party, has been created for the dominant purpose of adversarial litigation, this fact should, so far as possible, be recorded contemporaneously in the document (including expressly identifying the extant or contemplated litigation for which the document is being created). This will not create privilege in and of itself, but will help to identify privileged material and document the contemporaneous understanding of its privileged nature.

Working Papers Privilege

English legal privilege also extends to a lawyer's working papers. The justification for affording privilege protection to these materials has been said to be that their disclosure would be "giving [the party requesting disclosure] a clue as to the advice which had been given by the [lawyer] and giving them the benefit of the professional opinion which had been formed by the [lawyer.]"[118] The English Court of Appeal has elaborated on this justification, observing that "where the selection of documents which a [lawyer] has copied or assembled betrays the trend of the advice which he is giving the client the documents are privileged."[119]

[115] *Bilta (UK) Ltd. (in Liquidation) & Others v. (1) Royal Bank of Scotland Plc (2) Mercuria Energy Europe Trading Ltd.* [2017] EWHC 3535 (Ch).

[116] *Waugh v. Railways Board* [1980] AC 521 (HL) (in which it was held that the defendant could not show that anticipated litigation was the dominant purpose of the commissioning a report into the causes of a locomotive collision, but rather report was prepared for the "dual purposes" of ensuring safety on the railways and for obtaining legal advice on liability).

[117] *Re Highgrade Traders Ltd.* [1984] BCLC 151 (CA) (in which the Court of Appeal held that, although reports into the causes of a fire were held to be created for a "duality of purpose" (namely, to ascertain the causes of the incident and to obtain advice from lawyers), these purposes were "inseparable," with the result that litigation privilege would apply).

[118] *Lyell v. Kennedy* (No 3) (1884) 27 Ch D 1.

[119] *Ventouris v. Mountain* [1991] 1WLR 607.

Working papers privilege will not cover records taken by lawyers of information which itself would not otherwise covered by privilege.[120] Thus, to validly assert working papers privilege, there must be demonstrated some attribute of, or addition to, information which distinguishes the working papers from verbatim transcripts, or which reveals the trend of legal advice being given.[121] The fact that a "train of enquiry" (for example, the factual exchanges or information gathering processes which, although might provide the basis of the legal advice, do not reveal the trend of that advice) is revealed is not sufficient to give rise to working papers privilege.

CASE STUDY:
STAX CLAIMANTS V. BANK OF NOVA SCOTIA[122]

The English High Court contrasted a note which "records the substance of a conversation" (which would not be privileged) with a note which also records "the note-taker's own thoughts and comments on what he is recording with a view to advising his client" (which, the court said, almost certainly would be privileged).

Loss of Privilege

Waiver of Privilege

As with U.S. law, there are a number of contexts in which a company may inadvertently waive privilege. The general principle under English law is that a disclosure of privileged information to a third party constitutes a waiver of privilege as against the third party.[123] If disclosure to the third party (or third parties) results, additionally, in a loss of confidentiality in the material, then privilege may be lost in the material entirely.[124]

Moreover, where a party waives privilege over material, it may also be deemed to have waived privilege over other documents related to that issue where a failure to

[120] *Prop. All. Grp v. RBS* (No 3) [2015] EWHC 3341 (Ch).

[121] *The RBS Rights Issue Litigation* [2016].

[122] [2007] EWHC 1153 (Ch).

[123] *Mohammed v. Ministry of Defence* [2013] EWHC 4478 (QB).

[124] *Goldstone v. Williams, Deacon & Co.* (1899) 1 Ch 47.

disclose such documents means that the court and/or other parties would be given an incomplete picture of a particular issue. [125] This is known as the "cherry-picking" rule, and its effect is that, where a party discloses material related to an issue such that privilege is waived over that material, privilege is deemed to have been waived over all of the material relevant to the issue (a so-called "collateral waiver"). It should be noted that, for a collateral waiver to be engaged, a degree of reliance must be placed on the disclosed material by the disclosing party, for instance, by making use of the disclosed material in court.

Where privileged material is inadvertently disclosed, the party in receipt of the inadvertently disclosed material may utilize it in English proceedings only with the permission of the court,[126] although whether the court in fact restrains the use of such material is dependent on the circumstances. Urgent legal advice should be sought where privileged material has been inadvertently disclosed.

Limiting the Waiver of Privilege

In some circumstances, a limited waiver of privilege is recognized under English law, where privileged material is confidentially disclosed to a third party for specified purposes on the express or implied terms that privilege is not waived in the material.[127] Although, where material is shared on the basis of a limited waiver of privilege, residual privilege is retained by the disclosing party against the rest of the world, privilege is nevertheless waived as against the receiving party.

In the criminal or regulatory investigations context, it is not uncommon for organizations to seek to disclose material to U.K. authorities (whether voluntarily or under compulsion) pursuant to a limited waiver of privilege in an attempt to preserve privilege against third parties. The success of such a strategy will depend on the circumstances and, in some cases, for example, where the authority to whom the material has been disclosed is subject to onward disclosure obligations (for instance, to a defendant in contested proceedings), the authority may not be permitted (or

[125] *Nea Karteria Mar. Co. v. Atlantic & Great Lakes Steamship Corp.* (No 2) [1981] Com LR 138.

[126] Civil Procedure Rule 31.20.

[127] *USP Strategies v. London Gen. Holdings* [2004] EWHC 373 (Ch).

prepared) to agree to the terms of a limited waiver where the terms of such a limited waiver conflict with other disclosure requirements.

To the extent that material subsequently enters the public domain (for instance, in a criminal trial against a third party), confidentiality (and therefore privilege) will be lost notwithstanding any attempt to limit the waiver of privilege.

Where a document is being shared with a third party on the basis of a limited waiver of privilege, it should be recorded in writing that the document is being provided confidentially and on a limited waiver of privilege basis. This will not of itself ensure that the waiver of privilege is limited to the party receiving the document, it but will help to identify material over which privilege is retained.

France

Summary

Key issues:

— Under French law, legal privilege does not cover in-house counsel.

— Professional secrecy protects communications between an attorney and her client, but not correspondence with third-parties.

Protecting the Privilege:

— Professional secrecy is absolute in France; it cannot be waived, even upon the client's instructions.

— The protection of legal opinions and supporting documents is guaranteed by the professional secrecy of attorneys. Sensitive advice should be issued by external counsel who are members of a French Bar.

— The best way to shield sensitive content from disclosure is to keep it only at the offices of outside counsel.

Professional Duty of Secrecy

In France, the obligation of professional secrecy of attorneys ("*avocats*") covers both advice provided by counsel and any information, either written or oral, that was obtained in the course of the client's representation.[128] The secrecy covers: (i) communications between a client, and his or her attorney, (ii) correspondence between an attorney and his or her colleagues regarding representation of a client, with the exception of "official" correspondence, (iii) notes of meetings between attorney and client; and more generally, (iv) all related documents.[129] Only documents that are labelled "official" communications between lawyers are not covered by the professional secrecy.[130] Professional secrecy applies to civil matters as well as criminal investigations.[131] A breach of the duty of professional secrecy by an attorney is a criminal offense,[132] and it also constitutes professional misconduct.[133]

Exceptions to Professional Secrecy

Under French law, an attorney may reveal information otherwise protected by professional secrecy only to the extent that the disclosure is strictly necessary for the attorney's own defense before a jurisdiction.[134]

French law does not provide for an exception to professional secrecy akin to the crime-fraud exception under U.S. law.[135] Nonetheless, attorneys have an affirmative duty to report a suspicious transaction regarding possible money laundering activities and related criminal offenses by their clients whenever the reporting attorney knows, suspects, or has good reason to suspect, that a transaction or attempted transaction

[128] French Supreme Court, Civ. 1ère, 7 June 1983, n° 82-14469. In light of the limited disclosure obligations in French litigation, the notion of legal privilege is not recognized *per se* under French law. Judges have a discretionary power to order the production of a document, but only if it has been demonstrated that the requested document exists, is in the possession of the person from whom it has been requested, and is useful and essential to the action. Document discovery is thus extremely rare in French litigation, particularly because of the requirement that the requesting party specifically identify the document requested.

[129] Law 71-1130 of Dec. 31, 1971, Art. 66.5.

[130] Règlement Intérieur National de la profession d'avocat, Art. 2.2.

[131] *See* Law 71-1130 of Dec. 31, 1971, Art. 66.5; Code De Procédure Pénal (Criminal Procedure Code) C. Pr. Pén., art. 432.

[132] C. Pr. Pén, art. 226-13.

[133] Règlement Intérieur National de la profession d'avocat, art. 2.

[134] Decree n°2005-790 of 12 July 2005, art. 4 ; Règlement Intérieur National de la profession d'avocat, art. 2.1. Also *see* French Supreme Court, Crim., 29 May 1989, n° 87-82073.

[135] C. Pr. Pén. art. 434-1, which prohibits the concealment of felonies or misdemeanors, is not applicable to attorneys.

(i) is based on an offense that is punishable by more than one year's imprisonment, or (ii) is connected to terror financing.[136]

In addition, if the documents exchanged between the attorney and his client are covered by professional secrecy, an investigating magistrate cannot seize them[137] unless they are likely to demonstrate the attorney's participation in a criminal offense[138].

Professional secrecy protects communications between the attorney and his client but not correspondence with third-parties, which can be subject to wiretapping or seizure in the context of criminal investigations.[139] For example, the French Supreme Court held that professional secrecy does not extend to communications exchanged between the attorney and his client's certified public accountant.[140]

Waiver of Professional Secrecy

In France, professional secrecy cannot be waived. Attorneys may not disclose confidential information to any third party, even if authorized or requested by clients.[141] The client himself may, however, waive the benefit of professional secrecy by making public, for instance, a letter he sent to his lawyer.[142]

[136] French Monetary and Financial Code, art. L561-15, al. 1. This duty also extends to tax fraud when at least one objective criteria is present, as defined by decree. *See ibid.*, art. L. 561-15, al. 2 and D. 561-32-1. Also *see* Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. The report must be made to the president of the Bar ("*Bâtonnier*") exclusively.

[137] French Supreme Court, Com. 7 June 2011, n°10-18108.

[138] C. Pr. Pén., art. 56-1.

[139] French Supreme Court, Civ. 1ère, 10 Sept. 2014, n°13-22400 (in the context of communications between an attorney and a witness); French Supreme Court, Civ. 1ère, 31 Jan. 2008, n°06-14303 (exchanges between a party and his opponent's attorney).

[140] French Supreme Court, Com., 4 Nov. 2014, n° 13-20322.

[141] French Supreme Court, Civ. 1ère, 6 Apr. 2004, n°00-19245.

[142] French Supreme Court, Com., 6 June 2001, n° 98-18577.

In-house Counsel

In France, in-house lawyers ("*juristes d'entreprise*") have a different status from attorneys ("*avocats*"). Notably, in-house counsel do not bear a duty of professional secrecy and their communications are not covered by legal privilege.[143] In-house counsel who are not admitted to a French Bar cannot refuse to produce documents or give testimony.

[143] French Supreme Court, Civ. 1ère, 3 Nov. 2016, n° 15-20.495.

Germany

Summary

Key issues:

— Under German law, legal privilege does not attach to certain documents, but is instead closely connected with the attorney's right to refuse testimony.

— In-house counsel may refuse to give testimony only if their position and status within the company is comparable to that of an external attorney. This requires not only that the in-house counsel be admitted to the bar as a fully-qualified attorney, but also that the counsel's position in the hierarchy of the company grants a certain degree of independence.

Protecting the Privileges:

— All documents sought to be shielded from disclosure should be stored exclusively with counsel.

— The client's confidential files should be kept in the offices of their external counsel.

Professional Duty of Secrecy

Under German law, attorneys must maintain secrecy over any information they learn in the exercise of their profession, irrespective of its specific content. Likewise, the source of the information—whether counsel learned it from the client or from a third person—is irrelevant. As a consequence of this duty of secrecy, an attorney may, and is in fact obliged, to refuse to testify in court (civil as well as criminal cases) with regard to such information and to refuse to produce any documents that contain such information.[144] An attorney who breaches this duty can face criminal sanctions.[145] However, the testimony will still be admissible as evidence.

Attorneys can only be released from their duty of secrecy by their client.[146] The release can be granted expressly or by implication, for example by naming the attorney as a witness.

In addition to a release by the client, there are two main exceptions to the duty of secrecy. First, counsel may reveal information about their clients if they are themselves party to a dispute; [147] however, they may not reveal more than is necessary to support their case. Second, if the attorney learns that somebody is planning to commit a felony, an attorney is not only released from the duty of secrecy, but is obliged to report this to the relevant authorities and can face criminal charges for failure to do so.[148] However, the statute only lists particularly grievous felonies,[149] and for a duty to report, a person has to have valid reasons ("credible information") to believe that the crime will be committed. Lawyers are exempt from liability insofar as they learned about a planned felony in the exercise of their profession if they made an earnest effort to dissuade the potential perpetrator from committing the crime, or to avert the result, provided the felony in question does not fall within the categories of murder, genocide, crimes against humanity, war crimes, abduction, hostage taking, or an attack on air or maritime traffic by a terrorist organization.[150]

---

[144] Zivilprozessordnung (ZPO) [Code of Civil Procedure],§ 383(1) no. 6, Strafprozessordung (StPO) [Code of Criminal Procedure] § 53(1)1 no. 3.

[145] § 203(1) no. 3, § 204 StPO (Germany).

[146] If the client is a corporation, by its representative.

[147] For example, in disputes over the attorney's fees or in defense against claims for malpractice by the client.

[148] § 138 StPO (Germany). This duty exists for all citizens, and lawyers are not exempt.

[149] § 138 StPO (Germany).

[150] § 139(3) StPO (Germany).

Protection of Documents

Since privilege in the German sense is attached to the right to refuse testimony, attorney-client communications and other documents are only protected insofar as they are in the possession of a person entitled to refuse testimony (usually the attorney).[151] In general, aside from the attorney and his employees (see below), this applies to people who maintain a personal relationship with one of the lawsuit's parties (familial privilege), people who are under a duty of secrecy by virtue of their profession (professional privilege), or people who work as a public servant (public servants' privilege). Privilege may also arise out of the subject matter in question (subject matter privilege).[152] Documents in the possession of the client, whether prepared by an attorney or not, are generally not protected (again, however, it is important to note that the German civil process does not have extensive discovery or disclosure proceedings; this is therefore mainly relevant in the context of criminal investigations).[153] Likewise, while a lawyer may refuse to give testimony about information obtained from third parties, the third parties have no such right. This issue can become particularly relevant in the context of internal investigations: information obtained from interviewing employees in the course of internal investigations may be protected insofar as it is in the possession of the (external) attorney, who can refuse to disclose notes or give testimony; it can, however, be obtained from the interviewed employees.[154]

[151] The right to refuse testimony also applies to other persons who are under a duty of professional secrecy, such as doctors, as well as to clergymen, spouses, and relatives.

[152] David Greenwald and Marc Russenberger, *Privilege and Confidentiality: An International Handbook* 144 § 7.22 (2d ed. 2012).

[153] *See* generally, in criminal proceedings, however, communications between an attorney and client may not be seized even when in the possession of the client.

[154] In 2010, the Regional Court of Hamburg decided that an attorney's notes of interviews conducted with employees in the course of internal investigations are not protected, even if in the possession of the attorney (decision of Oct. 15, 2010, 608 Qs 18/10). However, following a legislative amendment, the Regional Court of Mannheim ruled in 2012 that all documents prepared in the course of internal investigations are protected as long as they are in the possession of an attorney (decision of July 3, 2012, 24 Qs 1/12). The Regional Court of Brunswick later held that documents from internal investigations created in preparation of the corporation's defense are protected regardless of whether they are in possession of the lawyer or the company (decision of July 21, 2015, 6 Qs 116/15). Since this topic is still under dispute, it is advisable to store any sensitive documents solely with the attorney.

CASE STUDY: RAID ON VOLKSWAGEN'S EXTERNAL COUNSEL

Recently, the Federal Constitutional Court, the highest constitutional court in Germany, found that seizure of documents relating to an investigation at external counsel's law offices did not violate the German constitution. Specifically, the Federal Constitutional Court held that Volkswagen AG, which was not the target of the particular investigation in question, had no recognized legal interest (*Rechtsschutzbedürfnis*) to assert a violation of the constitutional protection of the home against searches because the search was not conducted at VW's offices but at the law firm's premises. With respect to VW's constitutional right to informational self-determination (*Recht auf informationelle Selbstbestimmung*), which protects against extensive collection, storage, use, and processing of personal data, the Federal Constitutional Court acknowledged that the seizure of documents and their review could potentially impair VW's freedom of economic activities because a subsequent trial might reveal business and trade secrets to the general public or damage VW's reputation, but the seizure of documents was nonetheless deemed justified under constitutional law.

In particular, the Federal Constitutional Court found that documents exchanged between an individual or a company on the one hand and the defense lawyer on the other hand are only protected against seizure in cases in which the client, based on objective criteria, can reasonably be expected to become the subject of an investigation. The mere possibility or fear that criminal or administrative investigations against the client will be initiated is not sufficient. Since Audi AG, the target of this particular investigation, was not the client of the law firm, and VW was not targeted in the Munich investigation, the seizure of documents at the office of VW's law firm was deemed lawful. The Court confirmed that constitutional law does not protect a parent company from seizure of its documents on the grounds that its subsidiary is the target of an investigation. The Federal Constitutional Court noted, however, that the seized documents must not be used in an investigation directed against VW. According to the Federal Constitutional Court, constitutional law does not require reading statutory protections against seizure under the attorney-client privilege broadly, specifically because the public interest, in the effectiveness of law enforcement, acts as a counterweight.

In-house Counsel

Legal privilege applies only partially to in-house counsel. In-house counsel enjoys the right to refuse to testify only if their position and status within the company is comparable to that of an external attorney. This requires not only that the in-house counsel be admitted to the bar as a fully-qualified attorney, but also that the counsel's position in the hierarchy of the company grants a certain degree of independence. In addition, the right to refuse testimony can only be invoked insofar as the communications refer to legal advice as opposed to business advice, management tasks, or administrative tasks.

In-house counsel who are not admitted to the bar cannot refuse to produce documents or give testimony, as they are not formally attorneys. Even if they are admitted to the bar, the right to refuse to testify can only be invoked if in-house counsel is acting as independent counsel, not in its capacity as an employee.

Agents of Counsel

Personnel assisting an attorney (e.g., secretaries, law clerks, paralegals etc.) are also under a duty of secrecy and may therefore refuse testimony.[155] It is unclear whether this privilege extends to independent external service providers (e.g., detectives, expert witnesses).[156] The main criterion in this context is whether the external service providers can be regarded as assistants of the attorney in the case in question. As a rule of thumb, the more the attorney oversees, directs, and controls the work done by external agents, the more likely they will be regarded as falling within the legal privilege.

[155] This principle has recently been codified, *see* § 53a StPO (Germany) (right of professional assistants to refuse testimony); § 97(3) StPO (Germany) (protection from seizure extends to professional assistants); and § 203 StGB [Penal Code] (Germany) (disclosing information to professional assistants not a criminal offence).

[156] As opposed to court-appointed experts (who do not have the right to refuse testimony), whether expert witnesses appointed by one party enjoy this right is disputed. In this context, expert witnesses who are engaged by the attorney to facilitate the attorney's work likely fall within the attorney's right to refuse testimony.

Italy

Summary

Key issues:

— Legal privilege ("*Segreto professionale*") protects the confidentiality of attorneyclient communications and work product by lawyers.

— Legal privilege protects attorneys and their offices; clients may not themselves invoke privilege protection.

— Under Italian law, in-house counsel does not enjoy privilege rights.

Protecting the Privileges:

— Critical or material advice or memoranda should be issued by external counsel who are members of the Italian bar.

— Client's confidential files should be kept in the offices of external counsel.

— Correspondence should be marked with headers or footers signaling the existence of a legal privilege.

Professionals Entitled to Claim Legal Privilege

Italian legal privilege applies only to "qualified professionals" as defined in Article 200 CPP.[157] Qualified professional's include attorneys ("*avvocati*") who are members of the Italian bar. Italian legal privilege protects attorneys and their offices. Clients themselves may not invoke privilege to prevent search or seizure of correspondence or documents sent to or received from the attorney.[158] Pursuant to Article 200 Codes of Criminal and Civil Procedure ("CPP" and "CPC"), Italian attorneys have the right to abstain from testimony regarding any information acquired in connection with their activities. The privilege must be specifically invoked by the lawyer called as a witness, and it is subject to scrutiny by the court.[159]

Attorneys who are ordered to submit to a court client documents in their possession may refuse to do so on the grounds that such documents are confidential and relate to the attorney-client relationship. Similarly, inspections at the office of the defense counsel ("*difensore*") are permitted only where: (i) the attorney or those who work in his/her office are being prosecuted, (ii) the inspection is likely to uncover traces or other material evidence of the crime, or (iii) it is necessary to search for items or individuals identified in advance. In addition, attorneys also have the duty not to disclose the confidential subject matter of their professional services. Pursuant to Article 622 Criminal Code ("CP"), the violation of this duty can lead to criminal sanctions if the disclosure damages the client or a third party.[160]

[157] The scope of Art. 200 Cp.p. is narrow, and the list of professionals cannot be extended to include other similar professionals because, by virtue of Art. 200(1)(d) Cp.p., the right to claim professional secrecy can only be established by law. *See* Paolo Tonini, Manuale Di Procedura Penale, Giuffrè (2014) p. 297-98.

[158] While clients may not invoke privilege to prevent the search or seizure of correspondence or documents sent to or received from the attorney, this does not necessarily mean that any potentially privileged document in the client's possession must be disclosed, as documents may still be protected from seizure by the attorney if the attorney is present and objects to seizure.

[159] *See* Art. 200 C.p.p. ("1.The professionals listed below shall not be compelled to testify in court with respect to the confidential information they have knowledge of due to their [...] office or profession, unless they have a duty to report it to the judicial authorities:[...] (b) attorneys, private investigators, expert witnesses and notaries.").

[160] *See* Art. 622 C.p.p. ("anyone disclosing confidential information he or she acquired knowledge of due to his or her [...] profession, without cause or to gain profit for him or herself or for others, is punished, if such disclosure causes damage.").

Issues of Privilege Relating to Evidence in Italian Civil Litigation

In Italian civil litigation, issues of privilege relating to evidence and discovery may arise with regard to:

— Orders for production of documents (Article 210 CPC);

— Orders for inspection of persons or things (Article 118 CPC); and

— Right to refrain from giving testimony (Article 249 CPC).

Pursuant to Articles 118 and 210 CPC, upon request of a party to the proceeding, the court may order the other party or a third party to produce a document or other evidence, to consent to a physical search, or to consent to an inspection of an object in their possession if: (i) it is necessary to ascertain the facts of the case, and (ii) the enforcement thereof does not result in a breach of one of the duties of secrecy set forth by Articles 200 and 201 of the CPP.[161] Article 249 CPC also provides that the provisions of the Code of Criminal Procedure applicable to the hearing of witnesses (including art. 200 CPP) also apply to the civil proceedings. As a result of the interplay among Articles 210, 118, and 249 CPC and 200 CPP, a party to a proceeding or a third party called to testify or ordered to produce a specific document, or consent to an inspection, may refuse to do so on the basis of privilege.

Only minimal discovery is allowed under Italian law. Italian courts do not grant requests for the production of categories of documents or "any and all" documents relating to a defined legal relationship or other specific topic or request. Instead, Italian courts will grant discovery requests only for individual documents that are relevant and material to a dispute.[162] In addition, if a party fails to produce a

[161] Pursuant to Art. 118 at ¶¶ 2, 3, if the requested party refuses to comply with an order of inspection without cause, the court may draw adverse inferences against that party pursuant to Art. 116(2) C.p.c or order that the third party pay a fine ranging from Euro 250.00 to Euro 1,500.00.

[162] Supreme Court, judgment No. 3260 of Apr. 16, 1997; Supreme Court, judgment No. 26943 of December 12, 2007. The Supreme Court has recently affirmed that the order for document production is an evidentiary tool of last resort, which may be used only to obtain evidence that may not be obtained elsewhere. Supreme Court, judgment No. 4375 of Feb. 23, 2010.

document requested by the court, the court's recourse is limited to an inference that such document is adverse to the interests of that party.[163]

Legal Privilege Rights Under the Lawyer's Code of Ethics

In Italy, legal privilege is also protected by the Lawyer's Code of Ethics,[164] which imposes on lawyers a duty to respect professional secrecy. Applicable provisions stipulate, in relevant part, that a lawyer shall assure the rigorous observance of privilege and the utmost discretion regarding information received as part of the representation and any legal advice provided to the client.[165] However, a lawyer is allowed to disregard the duty of confidentiality in specific cases, such as when the disclosure of information would prevent the commission of a crime.[166]

Where an attorney violates his or her duty to respect professional secrecy, the National Legal Council[167] may issue pecuniary and disciplinary sanctions, including suspending the attorney from the exercise of the legal profession for one to three years.[168]

Legal Privilege for In-house Counsel

In 2012, Law 247/2012 regulating the legal profession in Italy (the "New Professional Law") came into effect, allowing in-house counsel to be also members of the Italian bar for the first time.[169] However, the New Professional Law does not explicitly grant legal privilege rights to purely inhouse counsel. Absent such an explicit provision,

[163] Claudio Consolo, Codice di Procedura Civile, Wolters Kluwer (2013) p. 2441.

[164] The Lawyer's Code of Ethics was approved by the National Legal Council on January 31, 2014.

[165] Art. 13 LCE. *See also* Art. 51 LCE at ¶ 1, pursuant to which, if a lawyer becomes a witness, he shall "refrain, unless in exceptional cases, from testifying as person of interest or witness about circumstances of which he has obtained information in the course of his professional activity or which are related to any representation in which he has been engaged."

[166] Art. 28 LCE at ¶ 4.

[167] The National Legal Council is a public institution which carries out, *inter alia*, administrative and disciplinary activities relating to the legal profession. It is established under the auspices of the Minister for Justice and consists of lawyers elected by their fellow members, with one representative for each appeals court district.

[168] Art. 28 LCE at ¶ 5. *See also* Art. 51 LCE at ¶ 4 ("The breach of duties under the previous sub-sections [*i.e.*, lawyer becoming a witness] entails the disciplinary sanction of censure.").

[169] The New Professional Law allows attorneys to work for an employer—either an individual person or a company—in the exclusive interest of such employer and under an employment contract, as long as the lawyer provides legal advice only on out-of-court transactions. Prior to its introduction in-house counsel did not enjoy any of the legal privilege rights that are applicable to members of the bar on the premise that they were employees of the company for which they work and could not be members of the Italian bar.

companies are well-advised to proceed on the understanding that inhouse counsel likely do not enjoy privilege rights.[170]

Waiver of Legal Privilege

Italian law does not expressly contemplate the waiver of legal privilege. However, absent specific provisions and case law, the existence of a waiver can be derived from Articles 622 and 50 C p. 253.[171] In practice, an attorney may implicitly or explicitly waive his or her right to legal privilege in several ways. For example, the privilege may be waived when the attorney: (i) does not claim the privilege at the time of the documents' request or seizure; (ii) voluntarily submits the documents to the court; or (iii) consents to the documents being seized.

Maximizing Protection of Confidentiality

In order to maximize the scope of privilege under Italian law, it is important to bear in mind some practical advice.

When seeking legal advice, it is advisable: (i) to enlist the assistance of external counsel who are members of the Italian bar; (ii) to issue powers-of-attorney or letters of appointment designating as counsel one or more external counsel; and (iii) to keep confidential files at the external counsel's offices. In documents prepared by external counsel, privileged correspondence should be marked with headers or footers signaling the existence of a legal privilege. Documents prepared by the client should clearly state that they were prepared in anticipation of an attorney-client communication for the purpose of obtaining a legal advice.

[170] *See* TAR Latium, judgment No. 7467 of Sept. 9, 2012. At the European level, this interpretation has been endorsed by the European Court of Justice in the judgment no. C-550/07 (*Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. European Commission*). However, scholars have argued that under article 6 of the European Convention on Human Rights, privilege also constitutes a fundamental personal right of the client that, consequently, is legally enforceable before the court. *See* Taru Spronken, Jan. Fermon, *Protection of Attorney-Client Privilege in Europe*, No. 2 Penn State International Law Review, Vol. 27, at 444.

[171] Art. 622 C.p. punishes anyone who discloses confidential information without cause or to gain a profit. Art. 50 C.p. provides that an individual infringing a right with the consent of the person entitled to dispose of such right does not commit a criminal offense.

Brazil[172]

Summary

Key issues:

— Legal privilege is a duty imposed upon lawyers, legal interns, and foreign law consultants. Clients may waive the privilege, but lawyers have an independent right not to testify in any lawsuit in which the attorney is or was a counsel, or in any lawsuit concerning any fact related to any current or former client.

— Legal privilege protects all information received by lawyers when representing their clients before judicial authorities, when performing any consultancy, or advisory activities, or when practicing as legal officers.

— Brazilian law makes no distinction between external and in-house counsel.

Protecting the Privileges:

— Records of communications between the client and lawyers cannot be admitted as evidence in court. However, the protection granted to the lawyers' workplace, work materials, and communications cannot act as a shield to criminal activities.

— Regardless of the clients' waiver, under civil and criminal procedures, even if authorized or requested by their clients, lawyers still have the right to refuse to testify on certain matters subject to privilege.

— Brazilian law does not provide for any specific rule about partial waivers. However, unless reasonably justified, the undue disclosure of confidential information obtained as a result of professional activities is considered a crime.

[172] Cleary Gottlieb does not practice Brazilian law, and the summary below is our high-level understanding of the current rules and practices in the country based on our experience and discussions with Brazilian counsel. It is not intended to provide, and should not be relied on as, legal advice. Readers should seek legal advice from Brazilian counsel on these matters.

The Privileges

Under Brazilian law, the attorney-client privilege is a right granted to both lawyers and clients and is a duty with which lawyers must comply. Lawyers must keep confidential all information obtained as a result of their legal practice.[173] This duty is owed not only by lawyers admitted to practice in Brazil, but also by interns who practice law under the supervision of attorneys,[174] and by foreign law consultants and foreign law consultancy firms registered before the Brazilian Bar Association (*Ordem dos Advogados do Brasil*).[175]

The duty of confidentiality applies to all information received by lawyers when representing their clients before judicial authorities, when performing any consultancy or advisory activities, or when practicing as legal officers.[176] Moreover, lawyers are bound by the duty of confidentiality when acting as mediators or arbitrators.[177]

Who controls the attorney-client privilege?

The attorney-client privilege belongs to both client and attorney. Brazilian law assumes that all communications and information exchanged between attorneys and their clients are confidential, regardless of any request by clients.[178] Unless an exception applies, such as those described below, any disclosure of information subject to privilege requires client's consent. Accordingly, to the extent information is protected by professional secrecy, lawyers cannot be compelled to testify about them in any civil, criminal, administrative, or arbitration proceedings.[179]

Brazilian law grants attorneys the right to refuse to testify in any lawsuit in which the attorney is or was a counsel, or in any lawsuit concerning any fact related to

[173] Brazilian Bar Association Ethics Code, art. 35.

[174] Federal Law no. 8,906/1994, art. 3, caput, and §3.

[175] Federal Board of the Brazilian Bar Association, Resolution no. 01/2010, art. 6 and art. 8.

[176] Brazilian Bar Association Ethics Code, art. 35, and Federal Law no. 8,906/1994, art. 1.

[177] Brazilian Bar Association Ethics Code, art. 36, §2.

[178] Brazilian Bar Association Ethics Code, art. 36.

[179] *See* C.P.P. (Brazilian Code of Civil Procedure), art. 448, II, and C.P.C. (Brazilian Code of Criminal Procedure), art. 207, and Brazilian Bar Association Ethics Code, art. 38. *See also*, e.g., Brazilian Supreme Court (Supremo Tribunal Federal - S.T.F.) (highest court of appeals on constitutional matters), HC no. 71039 /RJ, Relator: Min. Paulo Brossard, Tribunal Pleno, 7.4.1994, Diário da Justiça (D.J.), 6.12.1996, 48,708 (holding that witnesses subject to professional secrecy rules cannot be compelled to testify about information protected by those rules in any civil, criminal, or administrative procedures, nor in any testimony before parliamentary committees).

any current or former client, even if authorized or requested by such person, or in any lawsuit concerning facts subject to privilege.[180]

What information is protected under the attorney-client privilege?

The attorney-client privilege attaches to all information obtained by attorneys when performing legal activities.[181] Every communication between attorneys and clients is presumed to be confidential, regardless of any warning or request by either party.[182] This protection covers all written, electronic, or telephonic communications, as well as all information contained in attorneys' work materials and devices.[183]

Considering that all information gathered during the performance of legal activities is protected under the attorney-client privilege, Brazilian law does not make any distinction about the timing or specific purpose of the information disclosed by clients to their lawyers. In this regard, it is important to note that, even though Brazilian law does not provide for any protection similar to the U.S. work product doctrine, Brazilian civil procedure rules also do not provide for pre-trial discovery like that in the United States, and thus such work product protection is not as relevant.

However, the protection referred to above is granted only to the extent information is related to legal services provided by the attorney. Consequently, communications or information unrelated to legal activities, even if provided to a lawyer acting in other capacity, are not subject to privilege.[184]

Under what circumstances is the attorney-client privilege applicable?

Under Brazilian law, attorneys may not disclose confidential information to any third party except if authorized by clients.[185]

---

[180] Federal Law no. 8,906/1994, art. 7, XIX.

[181] Brazilian Bar Association Ethics Code, art. 35, and Federal Law no. 8,906/1994, art. 1.

[182] Brazilian Bar Association Ethics Code, art. 36.

[183] Federal Law no. 8,906/1994, art. 7, II.

[184] *See, e.g.*, Superior Court of Justice (Superior Tribunal de Justiça - S.T.J.) (highest court of appeals on all non-constitutional matters), Resp no. 1113734/SP (2009/0073629-9), Relator: Min. OG Fernandes, 6a Turma, 28.9.2010, Diário da Justiça Eletrônico (D.J.e.), 6.12.2010 (holding that, by recording an informal conversation between herself and an in-house counsel of the opposing party, one party did not violate any attorney-client privilege).

[185] Brazilian Bar Association Ethics Code, art. 35.

Special rules apply when attorneys are subpoenaed and called to testify in court. Pursuant to Brazilian civil and criminal procedure, lawyers cannot be compelled to testify about any information subject to privilege.[186] Moreover, even when privilege is waived by the client, attorneys still have the right to refuse to testify about any fact related to matters on which they worked or to any current or former client.[187] The attorney who refuses to testify has the discretion to determine whether the information is subject to privilege.[188]

Brazilian law grants lawyers a right to the sanctity of their work place, as well as a right to the confidentiality of any written, electronic, or telephonic communications between clients and lawyers, to the extent they are related to the exercise of the legal profession.[189] As a consequence, searches of lawyers' work materials and within their work places are not allowed.

How does the attorney-client privilege apply in the corporate context?

Outside and in-house counsel

With respect to the attorney-client privilege, Brazilian law makes no distinction between outside and in-house counsel.

Agents of counsel

Brazilian law does not address whether the confidentiality rules and the attorney-client privilege extend to agents who assist lawyers in the representation of clients. Still, if these agents are bound to professional secrecy rules imposed by their own profession (e.g., accountants, psychologists, and medical doctors), such rules apply regardless of the attorney-client privilege and are sufficient to prevent such professionals from being compelled to testify in civil and criminal procedures.[190]

[186] *See* C.P.C., art. 448, II, C.P.P., art. 207, and Brazilian Bar Association Ethics Code, art. 38. *See also, e.g.*, S.T.J., RHC no. 3946/DF (1994/0029831-5), Relator: Min. Adhemar Maciel, 6a Turma, 13.12.1994, D.J. 1.7.1996, 24,097 (holding that, if called as a witness, an attorney should appear in court, listen to the questions made by the court or by the opposing party, and then refuse to answer based on professional secrecy rules).

[187] Federal Law no. 8,906/1994, art. 7, XIX.

[188] *See, e.g.*, S.T.J., AgRg na APn no. 206/RJ (2001/0194801-5), Relator: Min. Cesar Asfor Rocha, Corte Especial, 10.4.2013, D.J., 4.8.2003, 202 (holding that it is up to the attorney to identify the information subject to privilege).

[189] Constituição Federal [C.F.] [Constitution], art. 133 (Braz.); Federal Law no. 8,906/1994, art. 7, II.

[190] *See* C.P.C., art. 448, II; C.P.P., art. 207.

What are the limitations to the attorney-client privilege?

Attorney-client privilege is not absolute under Brazilian law. Clients are entitled to waive their own privilege by disclosing or authorizing the disclosure of confidential information, and lawyers are not bound by professional secrecy rules when there is a severe threat to the attorney's life or honor, or when disclosure is necessary for the attorney's own defense.[191]

Additionally, the protection granted to the lawyers' workplace, work materials, and communications cannot act as a shield to criminal activities. Therefore, if there is evidence of crimes committed by lawyers, Brazilian law allows searches within their workplaces and seizure of their work materials. In this case, a search depends on a judicial warrant, must be witnessed by a representative of the Brazilian Bar Association, and is limited to the evidence pertaining to the attorney's involvement in criminal activities.[192]

When lawyers are involved in criminal activities and lose the protection that attaches to their work place and materials, searches may not comprise any document or object that belongs to the lawyer's clients (unless a specific client is involved in the same criminal activities as those of the lawyer).[193]

Likewise, if a search is conducted at the client's premises, it is also understood that any correspondence between client and lawyer cannot be seized or used as evidence (unless the lawyer has also been directly involved in the criminal activity). Generally, if there is evidence that a crime was committed by the client, a seizure of documents held by the client's attorney is nonetheless not allowed, unless such documents are considered to be *corpus delicti*, the foundation or material substance of a crime.[194]

A significant debate exists about whether records, interceptions, and wiretaps of communications between clients and their attorneys should be allowed as evidence during investigations of criminal activities involving the client. On one hand, the Brazilian Supreme Court (*Supremo Tribunal Federal*) has held that, as a general

[191] Brazilian Bar Association Ethics Code, art. 37.

[192] Federal Law no. 8,906/1994, art. 7, §6.

[193] Federal Law no. 8,906/1994, art. 7, §7.

[194] C.P.P., art. 243, §2.

rule, records of communications between the defendant and third parties can be admitted as evidence even if such communications were recorded by the defendant without the consent, or even without the awareness of the third parties involved. However, the Supreme Court also clarified that this rule does not apply to communications protected by professional secrecy rules, including those related to the attorney-client privilege.[195]

On the other hand, both the Brazilian Supreme Court (*Supremo Tribunal Federal*) and the Brazilian Superior Court of Justice (*Superior Tribunal de Justiça*) have recently held that there is no violation of the attorney-client privilege when wiretapping is carried out pursuant to Federal Law no. 9,296 of 1996, in circumstances where the client is the subject of the investigation, and interceptions are accidental[196] or there is evidence that, by rendering legal services, the attorney is also involved in criminal activities.[197] The Brazilian Bar Association disagrees with this view, and has recently decided to challenge the above mentioned decisions. A resolution has not yet been reached.[198]

[195] *See* S.T.F., Inq 4483/DF, Relator: Min. Edson Fachin, 30.8.2017, D.J.e., 12.9.2017 (holding that, in the context where defendants presented as evidence audio devices containing conversations recorded between them and third parties, and public prosecutors were later able to recover conversations that were deleted from the same devices before they were presented as evidence, conversations between such defendants and their attorneys should not be admitted as evidence).

[196] *See, e.g.*, S.T.J., AgRg no AREsp no. 457.522/SC (2014/0001937-6), Relator: Min. Rogerio Schietti Cruz, 6a Turma, 10.11.2015, D.J.e., 25.11.2015 (holding that the attorney-client privilege was not violated when a conversation between the spouse of the client and the attorney was intercepted during a lawful wiretapping procedure); S.T.J., REsp no. 1257058/RS (2011/0124761-0), Relator: Min. Mauro Campbell Marques, 2a Turma, 18.8.2015, D.J.e., 28.8.2015 (holding that there was no violation to attorney-client privilege as a result of a wiretapping procedure that accidentally caught a conversation with the client and her attorney, with no intention to investigate the lawyer's professional activities); S.T.J., RHC no. 26.704/RJ (2009/0169881-9), Relator: Min. Marco Aurélio Bellizze, 5a Turma, 17.11.2011, D.J.e., 6.2.2012 (holding that there was no violation to the attorney-client privilege by an incidental interception of a conversation between client and her lawyers during a wiretapping procedure).

[197] *See, e.g.*, S.T.J., RHC no. 51487/SP (2014/0231266-0), Relator: Min. Leopoldo de Arruda Raposo, 5a Turma, 23.6.2005, D.J.e., 24.9.2015 (holding that an attorney's telephone communications may be intercepted if there is evidence that she is involved in criminal activities); S.T.J., HC no. 210351/PR (2011/0141397-2), Relatora: Min. Marilza Maynard, 6a Turma, 19.8.2004, D.J.e., 1.9.2014 (holding that telephone communications between clients and lawyers may be intercepted if there is evidence that they are both involved in criminal activities as co-conspirators); S.T.F., HC no. 9609/MT, Relatora: Min. Ellen Gracie, 2a Turma, 17.11.2009, D.J.e. 232, 10.12.2009 (holding that telephone communications between clients and lawyers may be intercepted if there is evidence that the attorney is involved in criminal activities related to her legal activities); S.T.F., HC no. 106225/SP, Relator: Min. Marco Aurélio, 1a Turma, 7.2.2012, D.J.e 59, 21.3.2012 (holding that the attorney-client privilege cannot be used as a shield for criminal activities and that any information about criminal activities found in telephone communications lawfully intercepted may be used as evidence in criminal procedures).

[198] *See* Federal Board of the Brazilian Bar Association (Conselho Pleno do Conselho Federal da OAB), Proposição no. 49.0000.2017.005674-8/COP, 19.9.2017, D.O.U. de 21.9.2017, Seção 1: 183 (suggesting that the Brazilian Bar Association questions the Brazilian Supreme Court about the clients' rights to communicate in private and share confidential information with their attorneys).

Waivers of Privilege

Brazilian law asserts that clients are entitled to voluntarily waive their own privilege whether by disclosing confidential information to third parties or authorizing attorneys to do so. For instance, there is no violation of the attorney-client privilege when the client records their own conversation with their attorney and then uses it as evidence in future litigation (regardless of whether the attorney was aware that she was being recorded).[199]

Regardless of the clients' waiver, under civil and criminal procedures, even if authorized or requested by their clients, lawyers still have the right to refuse to testify on certain matters subject to privilege. Brazilian law does not provide for any specific rule about partial waivers, and there is no guidance on how lawyers should protect inadvertently disclosed confidential information. Notwithstanding the above, unless reasonably justified, the undue disclosure of confidential information obtained as a result of professional activities is considered a crime.[200] Such disclosure is also subject to discipline by the Brazilian Bar Association.[201]

[199] *See, e.g.*, S.T.J., RHC no. 48397/RJ (014/0125193-6), Relator: Min. Nefi Cordeiro, 6a Turma, 6.9.2016, D.J.e., 16.9.2016 (holding that conversations recorded by one of the persons taking part therein can be used as evidence in criminal procedures and do not violate attorney-client privileges).

[200] C.P., art. 154.

[201] Federal Law no. 8,906/1994, art. 34, VII.

Chapter V:
Data Privacy & Blocking Statutes

Summary

Key Principles:

— ***Broad scope***: The concept of what constitutes processing of personal data under European law is extremely broad.

— ***Processing requirements***: Personal data must be processed in accordance with principles of lawfulness, fairness, transparency, purpose limitation, data minimization, integrity, confidentiality, and accountability. Lawful processing requires consent or another legal basis provided for in EU or member states' national law. This can significantly limit a company's ability to produce personal data in the event of an investigation or other crisis.

— ***Employee monitoring***: More stringent restrictions apply to the processing of personal data in an employment context, especially when processing sensitive data.

— ***Transfer outside the EU***: Except in a limited number of circumstances, the transfer of personal data outside of the EU is only allowed to countries or organizations offering adequate protection, based on a decision of the European Commission, other appropriate contractual safeguards, or binding rules. Transfers to comply with a decision or order by a foreign court or administrative body require additional scrutiny.

Being Prepared:

— Identify all relevant jurisdictions where personal data is stored or processed and evaluate the legal grounds relied on for processing and transferring personal data.

— The GDPR has introduced significant changes, including with respect to transparency and consent requirements, data subjects' rights, regulatory oversight, and enforcement. Review data protection policies, monitoring policies, codes of conduct, and personal data inventories to ensure compliance and mitigate risks.

  - Include compliance and investigative processes as express purpose for data collection in privacy notices and internal policies.
  - Create robust ediscovery protocols and obtain the necessary approval such as from works council to simplify the process at the time of an investigation.
- Maintain a data privacy investigations and productions protocol, and be prepared to consult with local counsel as needed.

Introduction

In this chapter, we address data privacy and blocking statutes in two jurisdictions likely to be critical in any global crisis, the European Union ("EU") and Switzerland. Because these statutes raise complicated issues relating to the ability to process and transfer data, it is critical to consider these issues ahead of time, and to be prepared by taking certain pre-emptive steps designed to facilitate compliance with the rules and better position the company in the event of a crisis. Moreover, because the EU's new General Data Protection Regulation only went into effect in May 2018, it is important for companies to continue to update their analysis of the application of these statute as new guidance is provided by the authorities.

General Principles

Protection of personal data as a distinct fundamental right

In the European Union ("EU") both the right to respect each person's private life, home and communication ("privacy") and the right to the protection of personal data are recognized and protected as a fundamental individual rights. Article 7 of the EU Charter of Fundamental Rights (the "Charter") of 2000 protects the right to privacy and Article 8 of the Charter has elevated the protection of personal data to a specific and distinct fundamental right in the European Union and provides that the processing of personal data is prohibited, unless based on a legitimate basis

found in the law.[1] This fundamental right has also been repeatedly emphasized by the Court of Justice of the European Union ("CJEU").[2]

Until May 25, 2018, data protection within the European Union was governed by Directive 95/46/EC, adopted in 1995 (the "Directive")[3], which also established the advisory Article 29 Data Protection Working Party. As a directive under EU law, it left the implementation of the legal framework to the individual member state legislators[4], causing national data privacy laws in the European Union to have deviated to a certain extent.

Reform – GDPR

That situation changed as of May 25, 2018. On that date, the General Data Protection Regulation (EU) 2016/679 ("GDPR") replaced the Directive. As a regulation, it is binding in its entirety and directly applicable across all EU member states without the need for further national or local implementing implementation.[5] Although the general principles of the GDPR are broadly in line with the previously applicable legal regime, we will throughout this chapter highlight certain key differences and new concepts that need to be taken into consideration by companies that are active within the territorial scope of the GDPR. The GDPR also grants broader powers to the supervisory authorities, including the capacity to impose higher fines. For example, failure to ensure appropriate security of personal data or transferring personal data outside of the EU in violation of the GDPR can attract a fine of up to the higher of EUR 20 million or 4% of a company's total worldwide annual turnover.[6] As a result, companies must ensure compliance with the GDPR in connection with

---

1 Article 8(2) of the Charter.

2 CJEU Case C-553/07, *Rijkeboer*, EU:C:2009:293, § 47; C-291/12, *Schwarz*, ECLI:EU:C:2013:670; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, § 53; Case C-131/12, *Google Spain and Google*, EU:C:2014:317, §§ 53, 66 and 74; C-362/14, *Schrems*, ECLI:EU:C:2015:650; Joined Cases C-203/15, *Tele2 Sverige AB* and C-698/15, *Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

3 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Article 288 of the TFEU: "*a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States*" and "*a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.*"

5 Even though the GDPR leaves room for further implementation measures at national level in certain areas such as employment and processing of personal data of minors.

6 Article 83(5) GDPR. See also the Cleary alert memo on GDPR: The General Data Protection Regulation: Key Changes and Implications (https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/alert-memo-pdf-version-201650.pdf).

the transfer of any data, or risk significant penalties (although it remains to be seen how the GDPR is enforced in practice, of course).

Scope of Application of Data Privacy Rules

Broad Scope

The concept of "processing[7]" of data under European law is extremely broad and includes any action performed on that data, including, for example, merely storing it beyond the regular data retention, such as for a litigation hold.[8] What qualifies as personal data[9] may be as simple as an individual's name or email address (including business email), but may of course also encompass more sensitive information, which can trigger an even higher standard of protection.[10] Accordingly, European data privacy rules will apply to many of the actions necessary for an internal investigation or for responding to requests from public authorities in the event of a crisis, such as collecting data and reviewing it as part of an investigation.

The primary responsibility for compliance with data privacy laws when personal data is being processed resides with the "controller"[11], defined as "*the natural or legal person* [...] *which, alone or jointly with others, determines the purposes and means of the processing of personal data*." In the context of an internal investigation for example, the controller will usually be the company performing the investigation. When responding to governmental inquiries, it may become less clear who the

[7] Processing is defined as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*" (Article 2(b) Directive). Under GDPR, this definition will be slightly expanded to also cover structuring and restricting access to personal data (Article 4(2) GPDR).

[8] European data privacy laws apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2 GDPR). Data processing by public authorities themselves for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, is generally carved-out from the scope of the applicable privacy rules (Article 2(2) lit. d GDPR and future Directive (EU) 2016/680). But this carve-out does not apply to companies performing an internal investigation or cooperating with such public authorities.

[9] Personal data is defined as "*any information relating to an identified or identifiable natural person; an identifiable natural person or "data subject" is one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*" (Article 4(1) GDPR).

[10] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life are considered sensitive (Article 8(1) Directive). Under GDPR, this definition will be expanded to also cover genetic and biometric data (Article 9(1) GDPR).

[11] Note that unlike the current regime of the Directive, the GDPR does contain specific statutory obligations for processors, who will face directly liability concomitantly with the controller.

controller is, as many different actors can become involved and those entities may hold joint controllership.

Other parties typically involved in an investigation, such as external consultants and, under certain circumstances, even legal counsel supporting an internal investigation or the preparation of a response to regulator, will often be considered a "processor"[12], acting on behalf of the controller. The controller is not exonerated from liability under data privacy laws because the violation was committed by a processor on behalf of a controller. Data processors also have (increased) responsibility under the GDPR as, unlike with the Directive, the GDPR imposes direct legal compliance obligations on processors.[13]

DOCUMENTING PROCESSING BY EXTERNAL SERVICE PROVIDERS

Companies should be prepared to negotiate the legal terms and conditions of data processing agreements with external data processors, in particular in light of limitations of liability and hold harmless provisions concerning possible breaches of applicable data privacy laws. EU data privacy laws require that the relationship between the data controller and a data processor is governed by a binding written contract that sets out, among others, the subject-matter and duration of the data processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the parties in relation to the processing in sufficient detail.[14]

Territorial Scope

Unlike the Directive, which applied to processing carried out by companies either (i) established in an EU member state[15] or (ii) using equipment based in the EU, the GDPR has a significantly broader scope of application. The GDPR will apply extraterritorially to any internal investigation or preparation of a response to governmental requests that involves the processing of personal data of individuals who

[12] A "processor" is defined as "*a natural or legal person, public authority, agency or any other body which processes personal data* ***on behalf of the controller***" (emphasis added).

[13] Article 3 GDPR. These additional responsibilities for data processors include the implementation of technical and organizational measures, promptly notifying the data controller of any data breaches, and informing the data controller if the processor believes the instructions received from the controller are not GDPR-compliant.

[14] Article 28 GDPR.

[15] Or in a place where a member state's law applies by virtue of public international law.

are present in the EU, where the processing activities are related to monitoring of their behavior within the EU, irrespective of whether the company or data processor is established in the EU or whether or not the processing activities are performed in the EU.[16]

Processing Personal Data

What are the requirements for the processing of personal data?

Requirement of a legal basis

Personal data must be processed "l*awfully, fairly and in a transparent manner in relation to the data subject*".[17] A company processing personal data for purposes of conducting an internal investigation or responding to a governmental inquiry must ensure that a legal basis exists in order for it to be in complicate with data protection laws. The GDPR provides an exhaustive list of available legal bases, including consent by the data subject, compliance with a legal obligation, or performing a task carried out in the public interest, and the "legitimate interests" of the controller.[18]

Parties often gravitate towards consent from the relevant data subjects to justify processing as the seemingly simplest solution. However, this is often not the most expedient approach in the context of internal investigations or regulatory inquiries[19] because the requirements for consent are high and, even after consent is obtained,

[16] More broadly, the GDPR will apply to all controllers or processors established within the EU and processing personal data in the context of the activities, regardless of whether the data processing takes place in the EU or not (see also Article 3 GDPR).

[17] Article 5(1)(a) GDPR.

[18] See Article 6(1) GDPR, which broadly replicates the permissible grounds of the Directive. A legal basis exists if one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Member States may introduce specific provisions providing a legal basis for processing under national law. For companies processing "sensitive" personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, and genetic and biometric data, additional restrictions apply and the list of permissible grounds is even shorter, cf. Article 9 GDPR.

[19] It may often be impossible to contact all data subjects for practical or confidentiality reasons. Moreover, consent in the employer-employee context is seen as problematic by European Data Protection Authorities due to the imbalance of power inherent in the relationship, which calls the voluntary nature of such a consent into question. That consent must be freely given is however a key component. (See Article 29 Working Party, WP 249, 21).

it can be withdrawn by the data subjects at any time.[20] This would make any further processing unlawful and may also require the deletion of data that has already been processed.

Data processing by private entities in the context of investigations could be considered necessary either "f*or the performance of a task carried out in the public interest*" or "*for compliance with a legal obligation to which the controller is subject*".[21] The GDPR specifically mentions data exchanges in the context of competition law oversight, tax or customs administration, and financial supervisory authorities, and it is conceivable that cooperation in the context of an investigation with such global scope (such as the investigations relating to LIBOR, for example) could be considered to be in the public interest even for data transfers from private entities. However, the GDPR provides that these legal bases are narrowly interpreted. For example, the "legal obligation" has to be found in EU or member state law and could not for instance be based on a "*unilateral decision by a third country*," which suggests that responding to a subpoena from an authority outside of the EU, by itself is not a sufficient basis to process the data.

Outside of these exceptions, data processing may be permitted to the extent it falls within the company's "legitimate interests". To rely on this ground, the processing of personal data must be "*necessary for the purposes of the legitimate interests pursued by the company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data* [...]."[22] Whenever relying on this amorphous legal basis, companies must perform and document a true weighing and balancing of on the one side, their legitimate interests in processing personal data for compliance or investigative purposes (e.g., ensuring compliance with laws and/or avoiding civil or criminal sanctions, liability, negative publicity) and, on the other side, the fundamental rights of the individuals whose data is being processed (e.g., their right to privacy

[20] For guidance and analysis of the notion of consent under GDPR, see also Article 29 Working Party, WP 259, Guidelines on Consent under Regulation 2016/679.

[21] See Article 6(1) lit. e and c GDPR.

[22] See Article 6(1) lit. f GDPR. For external investigations, processing could be considered as "*necessary for the performance of a task carried out in the public interest*" pursuant to Article 6(1) lit. e GDPR. It is however unlikely that an internal investigation would, without more ado, qualify as a task carried out in the public interest, given that the basis for such interest must be laid down by EU or Member State law to which the investigator (as controller) is subject, cf. Article 6(3) GDPR. A unilaterally determined interest presented by a non-EU authority is therefore irrelevant. For private entities it is often not clear who makes the determination of what can be considered in the public interest. In both cases of either legitimate or public interest, the data subject has a right to object, cf. Article 21 GDPR.

and data protection). This balancing test is highly fact-based and must take into account such factors as the reasonable expectations of the individuals in relation to the privacy and security of their personal data, the nature and proportionality of the data processed, the principle of data minimization and purpose limitation as well as privacy-enhancing safeguards implemented by the parties involved (if any), all of which are discussed below.[23]

Data minimization

Personal data must be adequate, relevant and not excessive in relation to the purpose of the processing.[24] In short, this means that in the context of internal investigations or regulatory inquiries, companies may only process such types and amount of personal data as are strictly necessary to achieve the goals identified for the relevant internal investigation or governmental inquiry.[25] Note that data minimization also applies to any routine internal monitoring as well.[26] Under the GDPR, companies will also be required to carry out (and retain records of) an impact assessment for any data processing where the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*".[27] Such impact assessments on a voluntary basis can also be a valuable tool to demonstrate safeguards put in place to protect the data and data subject's rights.

Purpose limitation

Personal data may only be collected and processed for specific, explicit and legitimate purposes, and may not be further processed in a way that is incompatible with those initial purposes.[28] It is therefore key to provide appropriate provisions in the company's internal policies relating to the collection and storage of personal data (e.g., the email and use of mobile phone policies) that expressly allow for onward processing of the collected data for purposes of conducting internal investigations and responding to governmental requests.

---

[23] Article 29 Working Party, WP 217, p. 34 and 42.

[24] Article 5(1)(c) GDPR.

[25] Finding the right balance depends on various factors, such as the seriousness of the possible offense being investigated, the evidence already available, the stage of the investigation, and the expected impact on the affected individuals.

[26] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 23.

[27] Article 35 GDPR; see also Article 29 Working Party, WP 248 on Data Protection Impact Assessments and determining whether processing is "likely to result in a high risk" for the purposes of GDPR, which in the context of internal monitoring and internal investigations will have to be assessed on a case-by-case basis.

[28] Article 5(1)(b) GDPR; under GDPR, processing for a secondary purpose is permitted as long as it is compatible with the initial purpose of the data collection. Also, further processing for scientific research or statistical purposes is allowed.

Transparency and record keeping obligations

The GDPR increases transparency requirements, which has become an overarching data protection principle.[29] The data subject has the right to be notified of the processing of his or her personal data, the reason and legal basis for the processing, and whether data is to be transferred to a third country.[30] This can obviously create tension with the need for confidentiality in some circumstances.[31] Where the provision of information to a data subject would likely make it impossible to achieve the processing objectives, exemptions are available under certain circumstances.[32] In some cases, informing the data subject may even be prohibited, such as in connection with anti-money laundering ("AML") investigations, in which legislation makes it a criminal offence to inform an accountholder or a regulatory investigation.[33] In this situation, providing the data subject with information at the time of processing would obviously seriously impair the objectives of the legislation.[34]

Data controllers and processors are further under an express obligation under the GDPR to maintain adequate records of all processing activities, including in the context of internal investigations or regulatory inquiries.[35]

Rights of Data Subjects

As mentioned above, data subjects retain a number of rights under the GDPR, including rights of access and rectification, to object to processing.[36] Restrictions to these rights are permitted only under certain circumstances by EU law or at the

[29] Article 5 (1) a GDPR

[30] See Articles 12-14 GDPR. See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679.

[31] There are some other limited exceptions to this information obligation, for example, if providing such information proves impossible or would involve a disproportionate effort, see Article 14(5) GDPR. See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679.

[32] Article 14.5(b) and 23 GDPR. Exemptions may also be imposed by national Member State law, see recital 73 GDPR. One such example is Article 32 I of the French Data Protection Act 1978 which provides that data controllers are exempted from notifying data subjects when the "*processing of data is carried out for the purposes of preventing, investigating, identifying or prosecuting criminal offences*".

[33] See Article 39 of the 4th Anti-Money Laundering Directive (EU) 2015/849, implemented, for instance, in Sections 47 and 56(1) No. 60 of the German AML Act (*Geldwäschegesetz*), which provides for a fine up to EUR 5.000.000 under certain conditions. Article 55 § 1er and Article 81 § 6 of the respective Belgian *Loi du 18/09/2017 relative à la prévention du blanchiment de capitaux* [...] allows for administrative fines up to EUR 1.250.000 or 10% of the total annual net turnover, depending on the entity. Artt. 39, 55(4) of the respective Italian *Decreto legislativo 231/2007* as revised by *Decreto legislativo* 19/2017 allows the imposition of an up to one year's imprisonment or a fine up to EUR 30.000.

[34] See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679, 28. General information should be provided however to all account-holders when an account is opened that their personal data may be processed for anti-money laundering purposes.

[35] Article 30 GDPR.

[36] Data subjects' rights are covered by Chapter III of the GDPR; A company can deny a data subject's objection if it demonstrates compelling legitimate grounds which override the interests of the data subject or if the processing is necessary for the establishment, exercise or defense of legal claims (Article 21(1) GDPR).

national member state law level, such as in the context of prevention, investigation or prosecution of criminal offences.[37]

PRACTICE TIP:
RESPONDING TO DATA SUBJECTS' REQUESTS

Companies must consider how early they will handle data subjects exercising their rights and the need to implement systems and controls in order to ensure that they can easily track and rectify personal data, extract it and/or provide it to individuals in the required format when the need arises.

Ensuring the Security of Collected Data

Companies undertaking an internal investigation or preparing a response to a governmental inquiry that involves the processing of personal data must implement appropriate technical and organizational measures to ensure the security of the personal data processed, including protection against unauthorized or unlawful processing and against accidental breach, disclosure or loss.[38] Guaranteeing general IT system security and integrity, as well as data encryption, are the most evident measures. Access to any internal compliance monitoring data should in particular be strictly limited within an organization on a need to know basis. In addition, access logs should be maintained and access rights must be reviewed on a regular basis.[39]

Data Retention

Personal data collected for compliance or investigative purposes must not be kept in a form that allows identification of the individuals to whom the data relates for any longer than strictly necessary for this purpose. If a company implements a monitoring policy, it will need to ensure that any personal data obtained as a result of the monitoring remains accurate and up to date[40] and is not retained longer than necessary to satisfy legitimate legal or business needs.

---

[37] Article 23 (1) d. GDPR

[38] Article 5(1) lit. f GDPR.

[39] See, for example, the European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016), pp. 10-11.

[40] See Article 5(1) lit. d GDPR.

Employee Data Protection

While the Directive did not include employment-specific provisions, Art. 88 of the GDPR now makes specific reference to data processing in the employment context. In particular, the EU data protection authorities have pointed out on several occasions that relying on employees' consent to legitimize processing of their personal data is problematic, as the imbalance of power between an employer and employee calls into question whether such consent could ever be given "freely".[41] Employers will therefore often have to look to another legal basis to justify processing of employee data in the context of internal investigations or when responding to governmental requests and take the rights of the employee into consideration.

PRACTICE TIP:
POLICY ON USE MONITORING OF IT EQUIPMENT

Companies must draft and make accessible to employees a policy concerning the purposes for which, when, and by whom, suspicious log data can be accessed and to guide them about acceptable and unacceptable use of IT work facilities. It is also considered best practice to evaluate this policy at least annually to assess whether the chosen monitoring solution delivers the intended results or whether there are other, less invasive tools or means available to achieve the same purposes.[42]

These rules also apply to monitoring of electronic communications in the workplace, and employers must consider the proportionality of the measures they are implementing, and whether actions can be taken to mitigate or reduce the scale and impact of the data processing.[43] The European Court of Human Rights (the "ECtHR") has recently re-affirmed[44] that employers should provide employees with a prior notice of monitoring clearly indicating:

[41] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 6. The GDPR follows this approach and, in Recital 42, provides that "*consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*", while recital 43 adds that, "*in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller*"; see also Article 29 Working Party, WP 259, Guidelines on Consent under Regulation 2016/679.

[42] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 14. Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 14.

[43] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 4.

[44] *Bărbulescu v Romania* (ECtHR, Grand Chamber, Application No. 61496/08, 5 September 2017).

— the possibility that employees' communications might be monitored;

— the nature and the extent of the monitoring measures implemented; and

the employers' legitimate reasons justifying the introduction of the monitoring measures.[45]

PRACTICE TIP:
A WELL-DRAFTED IT AND MOBILE-PHONE AND PERSONAL DEVICES POLICY

— Make sure you have clear, readily accessible and (where necessary) country-specific policies in place indicating, *inter alia*, the permitted uses of company devices and other IT equipment including messenger services; if you allow employees to use their own devices to perform work (so-called "*Bring You Own Device*", "BYOD"), make sure your policies adequately address the issues raised in that respect.

— Make sure you have informed (and are able to demonstrate that you have informed) employees before any monitoring activity takes place of the possibility of the monitoring, its nature and extent and the legitimate grounds justifying the implementation of monitoring measures.

— Assess whether it is necessary to carry out a data protection impact assessment (a "DPIA"), due to the characteristics of the technologies involved and the circumstances of the specific personal data processing at stake.

— Assess whether the adopted monitoring measures constitute the least intrusive means to achieve the stated purposes.

Finally, one other point bears mention (and requires care) – there is a carve-out provision in the GDPR regarding data protection in the employment context that leaves the door open to national implementing laws, which may result in country-by-country differences.[46] This problem is exacerbated by the fact that violations

[45] *Bărbulescu v Romania* (ECtHR, Grand Chamber, Application No. 61496/08, 5 September 2017). In the ECtHR's view, theoretical reasons, by themselves, do not constitute an actual risk for the employer, and would not support the adoption of monitoring measures.

[46] GDPR, Article 88: "*Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment*". Indeed, in several matters, the GDPR allows Member States to discretionally introduce legislative provisions aimed at completing requirements of the GDPR or at derogating to such requirements. In Germany, for example, processing of employee data may also be lawful due to collective bargaining agreements and internal collective agreements.

of employee privacy rights are often criminally sanctioned in EU member states, sometimes even in the absence of criminal intent.[47]

Whistleblowing Systems

Because a whistleblower system may be the source of information that leads to an investigation or even a company-wide crisis, companies should be aware of the data privacy implications involved to avoid sanctions from the national data protection authorities or damage claims of data subjects.[48] Data obtained through any whistleblowing system should always be processed with the greatest confidentiality and a high level of data security through adequate technical and organizational measures.[49]

In order to comply with the GDPR, companies should be sure to limit the scope of possible recipients of the whistleblowing reports, ensure the security of the information processed in the system and, to the extent that other data subjects' avail themselves of their right to access, apply a multi-step procedure to inform the relevant individuals concerned at the right time about how and why their data is being processed.[50] Limited storage periods should be set and all staff informed of their rights[51], as a premature disclosure may, in the individual case, impair the success of an internal investigation. Likewise, in order to avoid abuse of the whistleblowing system, its purpose must be clearly defined in written internal policies and procedures.[52]

---

[47] By way of example, employers in Italy conducting video surveillance in the absence of a prior agreement with the trade union representatives may be subject to a fine up to EUR 1.549 or face an up to one year's imprisonment, which may be imposed cumulatively in the event of a serious infringement pursuant to Article 38(1) and (2) of the Worker's Statute (*Legge n. 300/1970*, as modified by *Decreti legislativi n. 196/2003* and *n. 151/2015*).

[48] This applies especially to "false positives", which shall refer to any person being falsely accused by a "whistleblower" and struggling, despite presumed or even duly proven innocence, to continue its career.

[49] See Article 32 GDPR.

[50] For further detailed recommendations (applied to EU institutions, but equally useful for private enterprises), see also the European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016).

[51] See, for example, Art. 15 GDPR ("*Right of access by the data subject*") *et seq.*

[52] See European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016), pp. 5-6 (see *supra*, Fn. 70).

In addition, national EU member state law can lay down additional rules on whistleblowing[53] and enact more rigorous restrictions.[54] In France, for example, whistleblowing hotlines that fall outside the scope of the French Data Protection Authority (CNIL)'s so-called Single Authorization No. AU-004 on whistleblowing schemes[55], must request a specific authorization from CNIL to be able to lawfully implement the hotline.

USING EVIDENCE GATHERED IN VIOLATION OF PRIVACY LAWS: EXAMPLE GERMANY

Evidence gathered in violation of the GDPR or the Federal Data Protection Act (*Bundesdatenschutzgesetz*, "BDSG") can be inadmissible in German court proceedings, even though a general "fruit of the forbidden tree" doctrine is not recognized in German procedural law.[56] In a recent decision, the German Federal Labor Court (*Bundesarbeitsgericht*) held that obtaining personal data by means of a keylogger from an employee which lead to the employee's dismissal could not be used as evidence, as the requirements of the legal basis for obtaining the data under German data protection law were not met.[57]

Finally, whistleblowing systems must comply with local employment laws. For instance, in Germany and France consultation with a "works council" is mandatory prior to implementing a whistleblowing procedure. In addition, some jurisdictions do not allow the use of evidence obtained from anonymous whistleblowing in court proceedings (a stance that in some cases may conflict with EU privacy legislation

[53] The legal landscape of whistleblower protection in the EU is still heavily fragmented. Some countries, such as the UK (*Public Interest Disclosure Act*, 1998), Romania (*Legea nr. 571/2004 privind protecția personalului din autoritățile publice, instituțiile publice și din alte unități care semnalează încălcări ale legii*, 2004), Slovenia (*Zakon o integriteti in preprečevanju korupcije (ZIntPK)*, 2010), Serbia (*Zakon o zaštiti uzbunjivača*, 2015) and France (*Loi Sapin II*, 2016) have adopted such rules, whereas other countries, including Germany, still lack a comprehensive whistleblowing framework.

[54] For example, Section 171(1) of the UK Data Protection Bill (as currently drafted) introduces a criminal offence of recklessly or intentionally re-identifying an individual from anonymized data (without the consent of the data controller), which may hinder the ability to whistle-blow. There are certain exemptions to the prohibition where the re-identification is carried out in the reasonable belief that it is justified in the public interest (Section 171(4)(c)(iii)), or where it is proved necessary for the detection of crime (Section 171(6)(a)).

[55] The CNIL Single Authorization, amended most recently on June 22, 2017 through CNIL Decision No. 2017-191, sets out detailed data privacy requirements that must be complied with by companies implementing a whistleblowing system in France and generally covers systems that allow the reporting of, among others, criminal offences, manifest and serious infringements of international commitments of France, manifest and serious violation of laws, serious threats to the public interest, and behavior contrary to the company's code of conduct on corruption or drug trafficking. It does not cover, for example, facts or matters protected by medical secrecy, legal privilege and/or national security confidentiality.

[56] German Supreme Court decision of June 30, 2005, case no. BvR 1502/04 – in German

[57] Decision of July 27, 2017, case no. 2 AZR 681/16, cf. http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=19516. – in German

requirements), and many jurisdictions do not allow an employer to contractually require an employee to "blow the whistle" and report on other employees.

Cross-border Transfers of Personal Data

In addition to the limitations described above with respect to processing data, additional restrictions apply to the transfer of personal data to countries outside of the European Economic Area ("EEA")[58] and specific safeguards need to be put in place. Companies should immediately begin considering these issues and familiarizing authorities and regulators outside of the EU with the issues raised by these limitations as soon as possible once an investigation begins.

Transfers within the EEA or to countries with an adequate level of protection

Cross-border transfers within the EEA are permitted provided they comply with the above-mentioned general requirements for processing personal data. Transfers of personal data outside the EEA may also be allowed where the European Commission has issued a so called adequacy decision finding that the third country provides an "adequate level of protection" (i.e., substantially equivalent to the level of protection offered in the EU).[59]

[58] As of the publication date of the present manual, the EEA consists of all 28 EU member states, plus Iceland, Norway and Liechtenstein. As regards the three latter states, the GDPR is currently under ongoing incorporation procedures into the EEA Agreement (see http://www.efta.int/eea-lex/32016R0679). Although Switzerland does not participate in this procedure, it is currently aligning its Data Protection Act to fulfill GDPR requirements.

[59] See Article 45 GDPR; http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. As of the publication date of the present manual, the Commission has recognized Andorra, Argentina, Canada (only for commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.

UK: POST-BREXIT CROSS-BORDER TRANSFER

Brexit (i.e., the UK's contemplated withdrawal from the EU) is likely to take the UK outside of the EU data protection legislative framework with the following key implications:

— **Third country status** – on January 9, 2018, the European Commission issued a notice to stakeholders[60] confirming that the UK will become a "third country" for data protection purposes once the UK has left the EU. In the absence of an adequacy decision from the European Commission, the transfer of personal data from the EEA to the UK will therefore need to be made subject to Appropriate Safeguards or data exporters will need to rely on the one of the Specific Derogations.

— **UK Data Protection Bill** – the European Commission notice to stakeholders did not indicate whether the UK will be considered "adequate" following Brexit. However, the UK has already signaled that it intends for UK legislation substantially to mirror EU data protection laws going forward in order to minimize disruption. It has therefore introduced a new draft Data Protection Bill in September 2017 according to which the GDPR shall apply "*as if its Articles were part of an Act extending to*" the U.K., subject to some adjustments for the post-Brexit term.[61] This bill, should it be passed, might facilitate the process of obtaining an adequacy decision for the UK after Brexit.[62]

— **Timing** – the UK is scheduled officially to leave the EU on March 29, 2019.

Transfers to countries without an adequacy decision by the European Commission

As a general rule, transfers of personal data outside the EEA to countries not covered by a European Commission adequacy decision are prohibited[63] in order to "e*nsure that the high level of that protection continues where personal data is transferred to a [non-EU state]*".[64] Recital 115 of the GDPR expressly states that "transfers "*should*

[60] European Commission Notice to Stakeholders on the withdrawal of the United Kingdom from the Union and EU rules in the field of data protection (http://ec.europa.eu/newsroom/just/redirection.cfm?item_id=611943).

[61] Draft Data Protection Bill 2017 as of September 14, 2017 (https://www.gov.uk/government/collections/data-protection-bill-2017).

[62] Extra-territoriality provisions in the GDPR will in any event require UK organizations providing services or monitoring the behavior of persons within the EU to comply with their requirements, regardless of their im-plementation in UK law.

[63] Article 44 GDPR.

[64] Case C-362/14, Schrems v. Data Protection Commissioner, ¶ 72, ECLI:EU:C:2015:650.

only be allowed where the conditions of this Regulation for a transfer to third countries are met."

If a company needs to transfer data out of the EEA to a country without an adequacy decision in the context of an internal investigation or governmental inquiry, either a specific legal derogation must be relied on[65], or an appropriate alternative safeguard as outlined in the GDPR must be put in place.[66]

What are possible derogations or appropriate safeguards to transfer data to an affiliated group company outside the EEA?

Specific Derogations. The GDPR enumerates certain specific situations in which data can be transferred to third countries, even in the absence of an applicable European Commission adequacy decision.[67] Explicit consent by the data subject is an option again, but the same concerns raised before apply to consent in the context of transfer. In particular consent may be withdrawn at any time, making future processing (and transfer) illegal.

A derogation is available when the transfer would be "*necessary for the establishment, exercise or defense of legal claims*".[68] However, tThe scope of this derogation is unclear. Traditionally this derogation was interpreted in some member states to apply to judicial proceedings only (e.g., for discovery purposes in U.S. litigation),[69] but there is little authoritative guidance on the interpretation of this derogation under the new provisions of the GDPR or, more generally, on the scope of this derogation in the context of internal investigations, voluntary disclosures to regulators, and governmental inquiries.

---

[65] See Article 49 GDPR.

[66] See Article 46-47 GDPR.

[67] The GDPR adds transfers that are "*necessary for compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject*" (Article 49(1) 2nd sentence). It is unclear how this approach will work in practice given the lack of guidance on the suitable safeguards required and the need to inform the relevant supervisory authorities of transfers made pursuant to this derogation. While the European Commission stated in its Brief on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15, that such interest could be recognized in "*not being subject to legal action in a non-EU state*", leading EU Data Protection And Privacy Scholars pointed out in their Brief as Amicus Curiae, p. 12, that "*a data controller's interest in complying with non-EU law is identical to an interest in not complying with the GDPR.*"

[68] See Article 49(1) lit. e GDPR. It is not clear yet how this interplays with the new Article 48 under the GDPR regarding judgments of foreign courts and decisions of administrative authorities (see below).

[69] Article 29 Working Party, WP 158, Working Document No. 1/2009 on pre-trial discovery for cross border civil litigation. Some member states such as Germany specified the claim requirements as "in court" in the national implementation of the Directive. These are no longer present in the harmonized GDPR text.

Appropriate safeguards. Another viable option to transfer data outside of the EEA, specifically in the context of internal investigations, is to put in place appropriate intra-group safeguards and ensure that enforceable protection of data subjects' rights and effective legal remedies are available. There are several ways to do this, including introducing binding corporate rules ("BCRs") at group level, having the relevant group entities enter into *ad hoc* contractual clauses based on the models adopted by the European Commission (or by a national data protection authority and approved by the Commission),[70] or adopting a specific data privacy tailored code of conduct,[71] or a certification mechanism[72] approved by the competent national data protection authority.

EU-U.S. Privacy Shield: adequacy based on self-certification. For companies based in the United States conducting an internal investigation or preparing a response to a governmental inquiry that also covers its European subsidiaries, the EU-U.S. Privacy Shield can offer a solution for *intra-group* data transfers or transfers to a data vendor. The Privacy Shield replaced the previously existing U.S. Safe Harbor scheme in July 2016, which was invalidated as a result of a legal challenge in EU courts.[73] Accordingly, U.S.-based companies may now elect to self-certify to the privacy principles set out in the Privacy Shield, and ensure compliance with those principles, in order to be authorized to transfer data from the EU to the US. While self-certification is relatively straightforward, monitoring compliance can be more difficult. The Privacy Shield passed its first review at the EU level, but legal challenges are pending.[74]

What are grounds to transfer data to governmental authorities outside the EEA?

The same means to transfer data that apply in an intra-group context would, in theory, also be available for (onward) transfers to a public authority. In practice,

[70] Where contractual clauses were authorized under the Directive as providing appropriate safeguards for the transfer of personal data to a third country, the GDPR provides that these authorizations will remain valid until amended, replaced or repealed (Article 46(5) GPDR).

[71] Based on the new scheme in Article 40 GDPR.

[72] Based on the new scheme in Article 42 GDPR.

[73] See also Article 29 Working Party, WP 238, Opinion No. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.

[74] The European justice commissioner and the Article 29 Working Party have also expressed the need for improvement of the Privacy Shield in some areas, in default whereof members of the latter announced bringing the Privacy Shield Adequacy decision to national courts to pave the way for a preliminary ruling of the CJEU. See, Article 29 Working Party, WP 255 on First annual Joint Review of the EU—U.S. Privacy Shield..

however, there are a number of additional complications that arise when personal data collected and processed within a corporate group is disclosed and transmitted outside of the group to public authorities. Adequate privacy-enhancing safeguards must be considered before transferring any personal data across borders to a court or other governmental authority, such as requesting a protective order in a litigation context (shielding the personal data from public disclosure)[75] or redacting documents for personal data (especially sensitive data) prior to any transfer.

Transfer to courts or administrative authorities. Article 48 of the GDPR, which specifically addresses disclosures ordered by non-EU states, provides that "*any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the third country and the Union or a Member State* [...]".[76] Article 48 of the GDPR expressly states that a request, for instance from a court in a third country, does not make a transfer legal, and indicates otherwise that mutual legal assistance treaties (MLATs) are the preferred transfer option given their "*carefully negotiated balance between the interests of different states* [...] *designed to mitigate jurisdictional conflicts*".[77] Of course, one issue with this approach is that it limits the ability to transfer data to those instances where such agreements have already been executed.[78] Further guidance from the data protection authorities and ultimately the Court of Justice of the European Union may be needed.

---

[75] Article 29 Working Party, WP 158, Working Document No. 1/2009 on pre-trial discovery for cross border civil litigation, p. 11.

[76] See Article 48 GDPR. See also recital 115 GDPR.

[77] See Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 14. The Article 29 Working Party recently underlined in a statement on e-evidence of November 29, 2017 that MLATs "*must—as a general rule—be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers. The circumvention of existing MLATs* [...] *is therefore an interference with the territorial sovereignty of an EU member state*." See also Brief of Jan Philipp Albrecht *et al.*, Members Of The European Parliament as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, pp. 18 *et seq.*, referring to European Parliament resolutions expressing concern over the circumvention of MLATs.

[78] See, for example, the MLAT in criminal matters between Germany and the US signed on October 14, 2003, whose bilingual version can be found in the Federal German Law Gazette, see http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl207s1618.pdf. In a written statement of January 31, 2007, Germany's Federal Ministry of Justice expressed its legal opinion on the precedence of this MLAT, see https://datenschutz-berlin.de/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2007-Web.pdf, pp. 186 *et seq.* Thus, seizure orders from US authorities directly addressed to private bodies in Germany are considered contrary to the Germany-US MLAT. Rather, pursuant to Article 1(5) *loc. cit.*, the German data protection authorities held the opinion that US authorities were at first required to "*request assistance pursuant to the provisions of this Treaty to obtain* [...] *documents, records, and other items*" in the German territory. Given the wording of Article 48 GDPR that applies "*without prejudice to other grounds for transfer pursuant to this Chapter*", it remains to be seen whether a voluntary transfer may also be permitted by virtue of Article 49 GDPR, irrespective of any official request for mutual legal assistance. The key issue remains a potential circumvention of existing MLATs (*see supra*, Fn. 101).

Finally, note that Article 48 applies "*without prejudice to other grounds for transfer pursuant to this Chapter*", so that the specific derogations afforded under Article 49 of the GDPR (described above) would still apply.[79]

Standard Contractual Clauses and internal safeguards not available. Companies will not be able to use the abovementioned Standard Contractual Clauses for transferring data to authorities, as the authorities will generally be unwilling or unable to enter into a binding contractual relationship with the company.[80] The group-internal specific safeguards, such as BCRs and codes of conduct, will likewise not be available in that situation.

"EU" public interest derogation. Apart from derogation for the establishment, exercise or defense of legal claims described above, which is primarily intended for use in the context of civil proceedings, the GDPR also provides a derogation for transfers necessary for important reasons of public interest[81], which more naturally applies in the context of law enforcement. It may be wise to assume that this derogation may be construed narrowly by European data privacy authorities and courts, such that only the interests identified as such by national legislation applicable to data controllers established in the EU will satisfy this "public interest" requirement (i.e., defined by EU or members state law under the supervisory jurisdiction of the CJEU).[82]

[79] See Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15.

[80] The Standard Contractual Clauses approved by the European Commission would for example claim to subject government agencies to the jurisdiction of EU data protection authorities and in the U.S. for example in many situations government authorities are prohibited from disclosing or granting further protection to certain personal information. See also David C. Shonka, *Cross Border Transfers—Producing Information from the EU to U.S. Government Agencies*, 17 DDEE 658 (2017).

[81] Recital 112 and Article 49(1) lit. d GDPR. See also Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15, referring to Article 83 TFEU stating particularly serious areas of crime.

[82] See Article 29 Working Party, WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, p. 15; this interpretation prevents circumvention by foreign authorities of the requirement for adequate protection and is currently supported by leading EU Data Protection And Privacy Scholars in their Brief as *Amicus Curiae*, United States v. Microsoft Corporation, 17-2, p. 11.

PRACTICE TIP:
SEDONA PRINCIPLES

The Sedona Conference (a nonprofit research and educational institute) regularly publishes guidelines and principles for addressing data protection in cross-border investigations, including in the context of government & internal investigations and on discovery, disclosure and data protection.[83] These principles are a useful resource for companies confronted with the issues described in this chapter.

Other Legal Restrictions

Other obstacles to data processing in the context of investigations can arise to varying degrees on a member state level.

France

In France, a Blocking Statute limits foreign discovery on French soil. Act 80-538 prohibits the communication of economic, commercial, industrial, financial or technical information to serve as proof in foreign administrative or judicial proceedings and imposes criminal sanctions for doing so. The prohibition covers French nationals, residents and officers, representatives, agents or employees of an entity with a head office or establishment in France. Such information may be communicated under limited circumstances, such as where the communication is permitted under French Law or an international treaty or agreement, such as the Hague Convention.[84]

In its guidance regarding data transfers for pre-trial discovery from July 2009, the French Data Protection agency CNIL expressly considers data transfers not in compliance with the Hague Convention "unlawful" under French data protection law.[85]

[83] See the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Gov-ernment & Internal Investigations: Principles, Commentary & Best Practices, May 2017; the Sedona Con-ference International Principles on Discovery, Disclosure & Data Protection – Jan 2017 Transitional Edition, January 2017.

[84] Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. 231.

[85] CNIL, Deliberation No. 2009-474 of 23 July 2009, concerning recommendations for the transfer of personal data in the context of U.S. court proceedings known as "Discovery."

Germany

In Germany[86], the Telemedia Act (*Telemediengesetz*, "TMG") and the Telecommunications Act (*Telekommunikationsgesetz*, "TKG"), both implement the ePrivacy Directive 2002/58/EC and seek, inter alia, (1) to protect the secrecy of telecommunications, safeguarded in Article 10 of the German Constitution, and (2) impose significant restrictions on the use of information sent through electronic communication. This may create additional obstacles for companies trying to obtain information stored on electronic devices used by personnel, in particular in the case of internal investigations of employees' private devices (BYOD). It is therefore important to set up a comprehensive corporate agreement on the business use of private equipment, and vice versa. Such a company agreement should grant control and access rights and state as accurately as possible whether screenings are done regularly or only in the event of doubt, and involve the co-determination of the works council. Failure to comply may result in administrative fines or criminal sanctions, such as an up to five years' imprisonment or a fine. Moreover, evidence gained from such violations may be considered inadmissible in court proceedings.

Other EU jurisdictions have similar restrictions in place in their respective ePrivacy Directive implementing measures, often also backed up by criminal sanctions.[87] In addition, obstacles to investigations and subsequent transfers may also arise from other areas such as labor law, professional or banking secrecy restrictions.

[86] See, *AccessData Corp. v. Alste Tech. GmbH*, 2010 WL 318477, Court for the District of Utah on January 21, 2010. The Court held that "*even assuming that* [Section 4c of the German Data Protection Act] *prohibited disclosure of personal third-party information, the United States Supreme Court has held* [in the Aerospatiale decision] *that '[i]t is well settled that such* [blocking] *statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute'*."

[87] See, for example, Article 145 of the Belgian Act on Electronic Communication of June 13, 2005.

PRACTICE TIP:
IDENTIFY RELEVANT JURISDICTIONS AND ENGAGE LOCAL COUNSEL EARLY

Companies should identify relevant jurisdictions and engage local counsel in those jurisdictions from the onset of any internal investigation or external investigation process that is subject to European data privacy laws. It is critical to understand where data is collected, where the individuals whose data is processed are located and which national laws apply.[88]

Swiss Data Privacy Rules and Blocking Statute

Federal Act on Data Protection

Swiss data protection laws are currently still governed by the Federal Act on Data Protection ("DPA") of June 19, 1992 (as amended), and the Federal Ordinance on Data Protection of June 14, 1993. Additionally, as in member states of the EU, data protection rules can be found throughout the legislative body of Switzerland, most notably the Swiss Federal Code of Obligations, which governs the processing of employee data in particular. A draft bill intended to adapt the Swiss federal Data Protection Act to reflect changes interlocked in the EU by the GDPR[89] as well as the amendments to Convention 108 has been proposed in September 2017.[90] That said, Swiss law employs concepts of personal data controller, processor, data subject and processing that are all similar to the GDPR. Failure to comply with the DPA provisions may lead to criminal sanctions and fines of up to CHF 250,000.

[88] See also Principle 1, Comment 1b of Sedona Conference International Principles for Addressing Data Pro-tection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p. 20; see also Cleary Gottlieb, "Selected Issues for Boards of Directors in 2018, 22, https://www.clearygottlieb.com/-/media/files/boards-of-directors-2018/selected-issues-for-boards-of-directors-2018-final-x2.pdf.

[89] The revised Swiss DPA further aims to pursue the goals of the (future) Police and Criminal Justice Authorities Directive 2016/680 because of the Schengen Agreement. The revised DPA will bring about amendments to other laws, inter alia to the Swiss Federal Penal Code and the Codes on Penal and Civil Procedure. For instance, the latter provides that court fees will not apply to court proceedings that concern the revised DPA.

[90] A preliminary draft has been issued on December 21, 2016.

PRACTICE TIP

The Swiss DPA is not applicable to data in international mutual legal assistance proceedings.

In the employment context, the employer owes employees specific care in Switzerland under the Code of Obligations in addition to the DPA, with regard to protecting the employee's rights. This restricts an employer's access to an employee's professional data.

Restrictions to data transfers out of Switzerland are similar to those in the EU. Certain countries are identified as providing adequate protection (EEA countries for instance), and there are safeguards that can be applied similar to in the EU (such as binding corporate rules, the Privacy Shield, and data transfer agreements). Article 6 of the current DPA[91] lists derogations that may apply outside of that, such as "*establishment, exercise, or enforcement of legal claims before the courts*" (Article 6, 2nd sentence, (d)[92]).

Blocking Statutes

In Switzerland two articles in « Crimes and Misdemeanors against the State and Defense » of the penal code protecting Swiss sovereignty and Swiss trade or business secrets against foreign requests can be pertinent to investigations.

First, Article 271 prohibits a foreign country from undertaking acts in Swiss territory that are in the competence of Swiss authorities, which includes the gathering of evidence for use in foreign proceedings (criminal, civil, or administrative). This may extend to remote access to such data as well. Data may only be collected through channels of judicial assistance such as the Hague Convention or MLATs.

Second, Article 273 prohibits disclosing third-party business secrets to foreign states and entities, without their consent. Third parties are include customers and business

[91] Article 13 of the latest draft bill.

[92] Article 14, 1st sentence, lit. c, (2) of the latest draft bill.

partners. The protected information must have a sufficient nexus to Switzerland to trigger Article 273. Disclosure through legal assistance proceedings is again possible. Violation of either Article carries a prison sentence or fine.

Key Steps to Prepare

— Companies should develop protocols addressing the production and transfer of information to authorities within reasonable timeframes. Companies should have a response team with data privacy experience that is prepared to deal with data processing and production questions on short notice.[93]

— When an authority is already involved in the investigation, companies should engage in a dialogue at an early stage regarding the gathering and transferring of data in order to make sure it is aware of EU data protection laws to communicate potential obstacles and potential delays.[94]

— Local counsel should be consulted early on to ensure compliance with local laws.

[93] See Principle 1 of the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p.19.

[94] See Principle 4 of the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p.24.

Chapter VI: Employee Rights and Privileges

Summary

Counsel and Coverage Issues

— Consider whether employees require separate counsel in any investigation or litigation involving the company.

— Frame by-laws carefully so as to consider to whom, and under what circumstances it will provide indemnification and advance fees to employees.

— There are restrictions on insured depository institutions limiting their ability to indemnify institution-affiliated parties in connection with bank regulatory proceedings.

Employment Actions

— Be vigilant of the circumstances under which they are prohibited from terminating employees, as well as of limitations on what they can say about an employee without incurring defamation risk.

— Sarbanes Oxley and Dodd-Frank provide protections to whistleblowers who file reports against their employers for violations of the securities laws. Companies should be cautious in how they craft language in employee agreements and how they address whistleblower concerns and should also keep the existence of whistleblowers in mind when considering whether to self-report potential violations.

— Carefully document the proper justifications for an employee's termination and be prepared to defend those justifications in follow-on legal proceedings.

Cross-border Concerns

— Consider cross-border differences in employee rights under local labor laws, privilege laws, data privacy concerns, and whistleblower rules.[1]

[1] For further discussion, *see* Chapter IV: Preserving Legal Privilege, and Chapter V: Data Privacy & Blocking Statutes.

Representation by Counsel of Companies and Employees

When determining whether the same attorney may represent a company and one of its employees, officers or directors, the company's attorney must consider whether its interests may conflict with the employee's interests. Both the prosecuting authorities and rules of professional conduct for attorneys require consideration of such conflicts and potential conflicts of interest, and particular caution is warranted in criminal cases. Under the ABA Model Rules of Professional Conduct, a "concurrent conflict of interest" exists where: "(1) the representation of one client will be directly adverse to another client; or (2) there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer."[2] The New York Rules of Professional Conduct similarly define a conflict as a situation where: "(1) the representation will involve the lawyer in representing differing interests; or (2) there is a significant risk that the lawyer's professional judgment on behalf of a client will be adversely affected by the lawyer's own financial, business, property, or other personal interests."[3]

If a conflict arises between the interests of the company and those of its employees, the same attorney cannot represent both the company and the individual employee unless: (1) the attorney believes she will be able to provide competent and diligent representation to both the company and the employee; (2) the representation is not prohibited by law; (3) the company and the employee do not assert claims against each other in the proceeding or litigation in which the attorney is representing both entities; and (4) both the company and the employee give informed consent, confirmed in writing.[4]

[2] Model Rules Prof'l Conduct r. 1.7(a) (Am. Bar Ass'n 2018).

[3] Rules Prof'l Conduct r. 1.7(a) (N.Y. State Bar Ass'n 2017).

[4] *See* Rules of Prof'l Conduct r. 1.7(b) (N.Y. State Bar Ass'n 2017); Model Rules of Prof'l Conduct r. 1.7(b) (Am. Bar Ass'n 2018).

PRACTICE TIP:
CONFLICTS OF INTEREST REQUIRING SEPARATE COUNSEL

- The company and employee assert claims against each other in the litigation, for example, if the company brings a cross-claim against the employee in connection with a third-party lawsuit brought against both the company and the employee or the company brings its own lawsuit against the employee based on the same underlying conduct.
- The attorney cannot diligently and competently represent both the company and the employee.
- The representation is prohibited by law.
- One or both parties do not give informed consent to the representation, confirmed in writing.[5]

Under the Model Rules of Professional Conduct, an unrepresented witness who has a conflict with the company may still be interviewed by counsel for the company, however the only advice company counsel is permitted to provide is that the unrepresented witness should secure counsel.[6] Where the company's counsel knows or should know that the organization's interests are adverse to the employee's interests, the company's counsel must explain that they represent the company, and not the employee,[7] and in fact, lawyers representing the company generally should inform the company's employees that they represent the company, and not individual employees (so-called "*Upjohn*" warnings).[8] Lawyers should further inform the employees that the conversation is privileged, but that the privilege belongs to the company, which can waive the privilege at its discretion. The failure to give such a warning creates a risk that the individual mistakenly believes the company lawyer represents her individually, and may prohibit the lawyer from disclosing information obtained in the interview.[9]

[5] Not all jurisdictions require consent to be in writing, but, notably, New York, New Jersey, and California do.

[6] Model Rules of Prof'l Conduct r. 4.3 (Am. Bar Ass'n 2018).

[7] Model Rules of Prof'l Conduct r. 1.13(f) (Am. Bar Ass'n 2018) .

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

[9] *See* Chapter IV: Preserving Legal Privilege.

Guidance issued by the Department of Justice ("DOJ") underscores the importance of these issues. The 2015 memorandum written by Deputy Attorney General Sally Yates titled "Individual Accountability for Corporate Wrongdoing" (the "Yates Memo") was written to guide DOJ attorneys when handling corporate matters. It emphasizes individual accountability and incentivizes companies to provide all relevant facts about individual employees involved in misconduct to the DOJ.[10] The Yates Memo has increased the importance of considering issues of separate representation and continually re-evaluating those decisions as a matter progresses.

During government investigations a company should carefully consider whether to obtain separate representation for individual employees. This will depend on a number of factors including: (1) the employee's right to have independent counsel; (2) the fact intensive nature of the inquiry (with counsel more appropriate for complicated matters than for simpler matters); (3) the nature of the conduct being investigated including whether there is a potential for criminal culpability; (4) the company's view of the employee including whether the employee is believed to have committed a crime against the company, or whether he is believed to have engaged in the conduct at issue in connection with the employee's business activities; (5) the need for expedition; and (6) whether external regulatory authorities have already begun to investigate (and the identity of those authorities), or whether the matter is purely internal. Other factors that may also be relevant include:

— For a company seeking cooperation credit, providing independent employee counsel can help to reassure the government that it will be able to obtain any relevant information it seeks from individuals without interference by the company. Individual employees may also be more willing to participate truthfully in interviews if they have their own counsel.

— Joint defense agreements between company and individual counsel must appropriately consider the objectives and stages of the government's investigation, and take care not to educate individual counsel or witnesses in ways that would interfere with the government's investigation.

[10] Deputy Att'y Gen. Sally Q. Yates, *Individual Accountability for Corporate Wrongdoing* at 1(Sep. 9, 2015) http://www.justice.gov/dag/file/769036/download.

As described in further detail in Chapter IV: Preserving Legal Privilege, companies should also be mindful of differences in privilege law in other jurisdictions when considering whether or not to undertake a joint representation with an employee of the company.

Corporate Obligations to Advance Attorney's Fees When Employees Face Legal Trouble

When a company employee requires separate representation in a civil, criminal, administrative, or investigative action, the company often pays for the employee's attorney's fees. In some instances, advancement of fees is required under provisions in its bylaws that mandate the advancement of such costs subject to repayment if it is subsequently determined that the employee is not entitled to be indemnified. In other instances, the company may choose voluntarily to advance attorney's fees. The scope of the right to advancement of attorney's fees is limited to the officer or director's entitlement under the company's advancement provision or bylaws. The bylaws may provide that advancement is subject to a prior good faith requirement, meaning that the employee acted in good faith and in a manner the person reasonably believed to be in or not opposed to the best interests of the company, or otherwise limit the right to advancement of expenses.[11] In contrast, bylaws may require the company to advance legal fees regardless of an employee's misconduct related to the underlying claims.[12]

[11] *Kaung v. Cole Nat'l Corp.*, 884 A.2d 500, 509 (Del. 2005) ("[T]he scope of an advancement proceeding under Section 145(k) of the [Delaware General Corporate Law] is limited to determining 'the issue of entitlement according to the corporation's advancement provisions and not to issues regarding the movant's alleged conduct in the underlying litigation'" (citation omitted)); *see also* 21 Marvin G. Pickholz, et al., *Indemnification and Advancement of Legal Fees*, 21 Sec. Crimes, § 4:23, n.18 (2d ed. 2017)("Advancement is not subject to a prior good faith requirement, unless that provision is specifically provided in the agreement.").

[12] *See, e.g., Miller v. U.S. Foodservice, Inc.*, 405 F. Supp. 2d 607, 618 (D. Md. 2005) ("[A] corporation may advance legal fees and expenses to an officer if the officer promises to repay the legal fees and expenses if the court ultimately does not find that he met the good faith requirement. Hence, while USF may later be entitled to a refund from Miller, nothing in the Delaware statute absolves USF from fulfilling its contractual obligation to pay Miller's reasonable legal fees and expenses as incurred."); *Pearson v. Exide Corp.*, 157 F. Supp. 2d 429, 438 (E.D. Pa. 2001) ("[U]nder the Bylaws, the alleged wrongful or *ultra vires* conduct of Pearson and Gauthier does not excuse Exide from satisfying its requirement to provide advancement of litigation expenses for which the plaintiffs are otherwise entitled."); *Tafeen v. Homestore, Inc.*, No. CIVA. 023-N, 2004 WL 556733 (Del. Ch. Mar. 16, 2004), *aff'd*, 888 A.2d 204 (Del. 2005) (noting that unclean hands related to the employee's actions that formed the basis of the underlying proceeding cannot be considered a defense for barring advancement, but unclean hands by the employee in intentionally sheltering assets before seeking advancement may be such a bar).

When Must a Company Advance Legal Fees For Its Employees in the United States?

In the United States, the largest number of corporations are incorporated under Delaware law, meaning the Delaware General Corporate Law ("DGCL") applies. The DGCL provides for both advancement of fees and indemnification. Advancement of fees refers to the payment of legal fees and expenses during pendency of the action.[13] DGCL section 145(e) allows corporations to provide advance payment of litigation expenses to officers and directors so long as the officer or director signs an undertaking to repay the corporation if she is not ultimately entitled to indemnification.[14] The corporation may advance litigation expenses to former officers or directors or other employees and agents of the corporation as the corporation deems appropriate.[15]

Where a corporation's bylaws are broadly written to require advancement of costs and fees to directors and officers, conditioned only upon the filing of an undertaking to repay such amount if it is determined that the director or officer is not entitled to indemnification, the corporation must advance such fees notwithstanding the permissive language of the DGCL.[16]

DGCL sections 145(a) and (b) give corporations the power to indemnify proceedings "by reason of the fact that the person is or was a director, officer, employee or agent of the corporation." Indemnification requires the ultimate outcome of the case to be decided.

---

[13] *See Kliger v. Drucker*, No. 003304/11, 2011 N.Y. Misc. LEXIS 6704, *20, (Sup. Ct. Nassau Cty. Oct. 13, 2011). Indeed, the purpose of advancement is to "provide[] corporate officials with immediate interim relief from the personal out-of-pocket financial burden of paying the significant on-going expenses inevitably involved with investigations and legal proceedings." *Sec. Exch. Comm'n v. FTC Capital Mkts.*, 09 Civ. 4755 (PGG), 2010 U.S. Dist. LEXIS 65417, at *14 (S.D.N.Y. June 29, 2010) (citing *Homestore, Inc. v. Tafeen*, 888 A.2d at 211).

[14] DGCL § 145(e) ("Expenses (including attorneys' fees) incurred by an officer or director of the corporation in defending any civil, criminal, administrative or investigation action, suit or proceeding may be paid by the corporation in advance of the final disposition of such action, suit or proceeding upon receipt of an undertaking by or on behalf of such director or officer to repay such amount if it shall ultimately be determined that such person is not entitled to be indemnified by the corporation as authorized in this section.").

[15] *Id*. ("Such expenses (including attorneys' fees) incurred by former directors and officers or other employees and agents of the corporation or by persons serving at the request of the corporation as directors, officers, employees or agents of another corporation, partnership, joint venture, trust or other enterprise may be so paid upon such terms and conditions, if any, as the corporation deems appropriate.").

[16] *Molyneux-Petraglia v. Northbridge Capital Mgmt., Inc.*, 841 N.Y.S.2d 219 (Sup. Ct. N.Y. Cty. Apr. 24, 2007); *see also Reddy v. Electronic Data Sys. Corp.*, No. CIV.A. 19467, 2002 WL 1358761, at *5 (Del. Ch. June 18, 2002) (executive employee was entitled to advancement of litigation expenses under the corporation's bylaws in connection with a criminal suit alleging conspiracy and mail and wire fraud and a related civil suit brought by the corporation during the performance of the employee's official duties as a manager).

Under Delaware law, if there is a nexus or causal connection between any of the underlying proceedings and one's official capacity, those proceedings are "by reason of the fact" that one was a corporate officer, without regard to one's motivation for engaging in that conduct.[17] For example, actions taken by a corporate officer in relation to separate shell companies set up by the corporation for the purpose of facilitating a tax shelter transaction were "by reason of the fact" that the person was a corporate officer.[18] A nexus or causal connection exists where, but for the person's role in the corporation, he or should would not have been involved in the action at issue.[19]

Other states have different indemnification and advancement rules. For example, in New York, New York Business Corporation Law §§722-24 governs the advancement of attorney's fees and costs.[20] In New York, indemnification is not available to a director or officer if a judgment or final adjudication is entered against the director or officer which establishes that: (1) his acts were committed in bad faith, or were the result of active and deliberate dishonesty and were material to the cause of action, or (2) he personally gained a financial profit or other advantage to which he was not legally entitled.[21]

When is an Undertaking Required?

An undertaking is required for advancement of fees and costs. Before the corporation advances attorney's fees and costs for the defense of an action, the individual employee must provide the corporation with an undertaking. An undertaking is an

[17] *Homestore,* 888 A.2d at 214; *Perconti v. Thornton Oil Corp.*, No. Civ .A. 18630–NC, 2002 WL 982419, at *3-4 (Del Ch. May 3, 2002); *Molyneux-Petraglia*, 841 N.Y.S.2d at 2.

[18] *Molyneux-Petraglia*, 841 N.Y.S.2d at 2.

[19] *Id*.

[20] N.Y. Bus. Corp. Law § 722(a) (2018) ("[A] corporation may indemnify any person made, or threatened to be made, a party to an action or proceeding (other than one by or in the right of the corporation to procure a judgment in its favor), whether civil or criminal, including an action by or in the right of any other corporation of any kind . . . which any director or officer of the corporation served in any capacity at the request of the corporation . . . in good faith, for a purpose which he reasonably believed to be in . . . [and] had no reasonable cause to believe that his conduct was unlawful").

[21] *Id*. at § 721 ("The indemnification and advancement of expenses . . . shall not be deemed exclusive of any other rights to which a director or officer seeking indemnification or advancement of expenses may be entitled, whether contained in the certificate of incorporation or the by-laws or, when authorized by such certificate of incorporation or by-laws, (i) a resolution of shareholders, (ii) a resolution of directors, or (iii) an agreement providing for such indemnification, provided that no indemnification may be made to or on behalf of any director or officer if a judgment or other final adjudication adverse to the director or officer establishes that his acts were committed in bad faith or were the result of active and deliberate dishonesty and were material to the cause of action so adjudicated, or that he personally gained in fact a financial profit or other advantage to which he was not legally entitled."); *see also id*. § 722(c) (indemnification of officers and directors in derivative actions).

unconditional, unsecured promise by the officer or director to repay the advance to the corporation. No deposit, bond, or security is required.[22]

When Is Advancement of Fees Advisable?

Advancement of attorney's fees may help attract capable individuals into corporate service by easing the financial burden of paying personal out-of-pocket expenses involved with investigations and legal proceedings.[23] This "allows corporate officials to defend themselves in legal proceedings, secure in the knowledge that, if vindicated, the corporation will bear the expense of litigation."[24]

Can Advancement of Fees Be Used As Evidence Against the Corporation?

The U.S. government cannot hold advancement of fees to individuals as evidence against a company in a criminal proceeding.[25] In *United States v. Stein*,[26] KPMG was accused of developing, marketing, and implementing abusive tax shelters. Federal prosecutors were investigating potential criminal conduct by employees of KPMG, and KPMG originally adhered to its long-standing policy of paying the attorney's fees of its employees in defending against these accusations. Federal prosecutors, in making the decision on whether to charge KPMG with a crime, adhered to the Thompson Memo, which was issued in 2003 by then Deputy Attorney General Larry Thompson.[27] The Thompson Memo was written to help federal prosecutors decide whether to charge a corporation, rather than or in addition to individuals within

---

[22] *See, e.g., Spitzer v. Soundview Health Ctr.*, No. 401432/04, 2005 N.Y. Misc. LEXIS 3249, at *9 (Sup. Ct. N. Y. Cty. Jan. 27, 2005); *see also* DGCL § 145(e).

[23] *Schlossberg v. Schwartz*, 992 N.Y.S.2d 161, at *10 (Sup. Ct. Nassau Cty. May 14, 2014) ("[O]ne of the beneficial purposes behind advancement is to help attract capable individuals into corporate service by easing the burden of litigation-related expenses. In particular, advancement provides corporate officials with immediate interim relief from the personal out-of-pocket financial burden of paying the significant on-going expenses inevitably involved with investigations and legal proceedings.") (quoting *Ficus Invs., Inc. v. Private Capital Mgmt.*, 61 A.D.3d 1 (1st Dep't 2009) (quotation marks omitted).

[24] *Molyneux-Petraglia*, 841 N.Y.S.2d at 3 (citation omitted); *see also* DGCL § 145(c) ("To the extent that a present or former director or officer of a corporation has been successful on the merits or otherwise in defense of any action, suit or proceeding referred to in subsections (a) and (b) of this section, or in defense of any claim, issue or matter therein, such person shall be indemnified against expenses (including attorneys' fees) actually and reasonably incurred by such person in connection therewith.").

[25] *United States v. Stein*, 435 F. Supp. 2d 330 (S.D.N.Y. 2006), *aff'd*, 541 F.3d 130 (2d Cir. 2008); *see also* Deputy Att'y Gen. Mark Filip, *Principles of Federal Prosecution of Business Organizations* (Aug. 28, 2008), https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf ("2008 Filip memo").

[26] *United States v. Stein*, 435 F. Supp. 2d 330 (S.D.N.Y. 2006).

[27] Deputy Att'y Gen. Larry D. Thompson, *Principles of Federal Prosecution of Business Organizations* (Jan. 20, 2003), https://www.americanbar.org/content/dam/aba/migrated/poladv/priorities/privilegewaiver/2003jan20_privwaiv_dojthomp.authcheckdam.pdf ("Thompson Memo").

the corporation, with criminal offenses. Under the 2003 Thompson Memo, "the corporation's willingness to identify the culprits within the corporation, including senior executives," was a consideration when determining whether a company will receive cooperation credit.[28] The Thompson Memo noted that "[a] factor to be weighed by the prosecutor is whether the corporation appears to be protecting its culpable employees and agents."[29] Thus, under the Thompson Memo, one factor the government took into account in measuring the corporation's overall cooperation was whether the corporation promised to support culpable employees and agents by advancing attorney's fees.

After the government informed KPMG that adherence to its policy of indemnifying attorney's fees would weigh against it when determining whether to prosecute, KPMG informed employees that: (1) it would move forward with paying legal fees only if these employees forfeited their Fifth Amendment right to remain silent in order to fully cooperate with the government investigation, (2) legal representation was not required to speak with investigators, and (3) KPMG would cease paying legal fees if the employee was criminally charged. This led to the denial of legal fees for many employees and the termination of others. The *Stein* court held that the government, through the actions of the prosecutors and the directives within the Thompson Memo, violated the Fifth and Sixth Amendment rights of individual defendant-employees.

In 2008, the Filip Memo, issued by then Deputy Attorney General Mark Filip, outlined what measures a corporate entity must undertake to qualify for "cooperation" credit.[30] The Filip Memo sets out that the government can no longer consider whether a company advanced attorney's fees to employees or entered into a joint defense agreement when deciding whether to charge the company with wrongdoing.[31]

[28] *Id*. at 6.

[29] *Id*. at 7.

[30] *See* 2008 Filip Memo.

[31] Carol A. Poindexter & Norton Rose Fulbright, *Criminal and Civil Liability for Corporations, Officers, and Directors*, Practice Note 6-501-9459, West Practical Law (database updated July 2018).

The Yates Memo mentioned above did not change the DOJ's policy on advancement of attorney's fees. However, because the Yates Memo increased the importance of separate representation for individual employees, corporations, as a result, may be more likely to advance attorney's fees for employees.[32]

When Can the Corporation Claw Back Advanced Fees?

DGCL § 145(e) provides that if the director or officer is deemed not to be entitled to indemnification, the corporation may claw back advanced fees pursuant to an undertaking signed by or on behalf of the director.[33] The corporation must wait until the final disposition of the proceedings to claw back any advanced fees if the director or officer is not entitled to indemnification.[34]

Director and Officer Insurance for Corporate Indemnification Obligations

The goal of D&O insurance is to protect directors and officers from losses suffered as a result of their service to the company.[35] A company may also purchase insurance to cover the amounts it has to indemnify its directors and officers.[36]

A D&O policy typically consists of three potential coverages:

— **Side A coverage:** This coverage indemnifies individual directors and officers for losses for which they are not indemnified by their corporation.

— **Side B coverage:** This coverage reimburses the corporation for amounts that it is lawfully permitted or required to expend in indemnifying its officers and directors for their losses.

---

[32] *See* Yates Memo.

[33] *See* DGCL § 145(e) ("Expenses . . . may be paid by the corporation in advance of the final disposition of such action, suit or proceeding upon receipt of an undertaking by or on behalf of such director or officer to repay such amount if it shall ultimately be determined that such person is not entitled to be indemnified by the corporation as authorized in this section.")

[34] *Bergonzi v. Rite Aid Corp.*, No. Civ. A. 20453-NC, 2003 WL 22407303, at *2 (Del. Ch. Oct. 20, 2003) ("As Bergonzi is entitled to advancement until a final disposition of the proceedings, and as the proceedings have not yet reached a final disposition, Bergonzi has a presently enforceable right to advancement. Advancement is a right that the Supreme Court has recognized as distinct from the right to indemnification." (citation omitted)).

[35] Helen K. Michael, Virginia R. Duke & Kilpatrick Townsend & Stockton LLP, *Directors and Officers Liability Insurance Policies*, Practice Note 2-504-6515, West Practical Law (database updated Feb. 2011).

[36] *Id*.

— **Side C coverage:** This coverage is for the entity itself. It generally covers securities actions and protects the corporation for its own liabilities.[37]

Whistleblower Protections for Employees

U.S. Whistleblower Protections Under the Sarbanes-Oxley Act

Sarbanes-Oxley § 806, 18 U.S.C. 1514A, contains significant whistleblower protections and requires companies to implement controls to identify and prevent fraud. Sarbanes-Oxley's whistleblower protections cover not only federal employees, but also employees of publicly-held companies.

A person who alleges discharge or discrimination by any person in retaliation for blowing the whistle, may seek relief by either: "A) filing a complaint with the Secretary of Labor; or B) if the Secretary of Labor has not issued a final decision within 180 days of the filing of the complaint and there is no showing that such delay is due to the bad faith of the claimant, bringing an action at law or equity for de novo review in the appropriate district court of the United States."[38] The district court in which such an action is brought has subject matter jurisdiction, regardless of the amount in controversy. The statute of limitations is 180 days after the date when the violation occurs.[39] Sarbanes-Oxley entitles the employee to relief necessary to be made whole, meaning a successful claim can result in reinstatement and back pay with interest.[40]

U.S. Whistleblower Protections Under Dodd-Frank

Dodd-Frank, 15 U.S.C. § 78u-6, goes beyond Sarbanes-Oxley to provide more expansive protections to statutory whistleblowers.[41] Under Dodd-Frank, a whistleblower is defined as: "any individual who provides, or 2 or more individuals acting jointly who provide, information relating to a violation of the securities laws to the

[37] Gary Lockwood, *Structure of D&O policies, Law of Corp. Officers & Dir.: Indemn. & Ins.*, § 4.8 (2d ed. 2017).

[38] 18 U.S.C. § 1514A(b)(1) (2018).

[39] 18 U.S.C. § 1514A(b)(2) (2018).

[40] 18 U.S.C. § 1514A(c)(2)(A)-(C) (2018).

[41] Jill L. Rosenberg & Renee B. Phillips, *Whistleblower Claims Under the Dodd-Frank Wall Street Reform and Consumer Protection Act: The New Landscape*, https://www.nysba.org/Sections/Labor_and_Employment/Labor_PDFs/LaborMeetingsAssets/Whistleblower_Claims_Under_Dodd_Frank.html.

Commission, in a manner established, by rule or regulation, by the [Securities and Exchange] Commission."[42]

Dodd-Frank creates a private right of action for anti-retaliation protection.[43] An individual alleging retaliation can file suit directly in federal court; unlike under Sarbanes-Oxley, there is no requirement that an individual first file a complaint with the Secretary of Labor. The statute of limitations is six years after the date when the retaliation occurs or within three years after the date "facts material to the right of action are known or reasonably should have been known by the employee" but not more than "10 years after the date the violation occurs."[44] Under Dodd-Frank, the Securities and Exchange Commission ("SEC" or "Commission") may also initiate a retaliation suit. A successful retaliation claim can result in reinstatement, double back pay, and attorney's fees and costs.[45]

Until recently, courts were divided on whether the scope of Dodd-Frank's anti-retaliation provision exclusively covered whistleblowers who report directly to the SEC or whether it also applied to individuals who only report internally.[46] On February 21, 2018, in *Digital Realty Trust v. Somers*, the Supreme Court held unanimously that Dodd-Frank's anti-retaliation provision applies only to whistleblowers who report their claims to the SEC, and internal reporting alone does not trigger Dodd-Frank's protections against retaliation. The Court's decision may lead to an increase in SEC whistleblower claims because the law is now clear that external reporting is required to take full advantage of Dodd-Frank's whistleblower protections.[47]

The Supreme Court's *Digital Realty* decision does not necessarily change how companies should address internal-reporting practices or whistleblowers, as one

---

[42] 15 U.S.C. § 78u-6(a)(6) (2018).

[43] 15 U.S.C. § 78u-6(h)(1)(A) (2018).

[44] 15 U.S.C. § 78u-6(h)(1)(B)(iii) (2018).

[45] 15 U.S.C. § 78u-6(h)(1)(C) (2018).

[46] *Compare Egan v. TradingScreen Inc.*, No. 10 Civ. 8202 (LBS), 2011 WL 1672066, at *4 (S.D.N.Y. May 4, 2011) (holding that Dodd-Frank's anti-retaliation provision covers not only whistleblowers who provide information to the SEC, but also individuals whose "disclosures that are required or protected under [Sarbanes-Oxley] . . . the Securities Exchange Act of 1934, [18 U.S.C. § 1513(e)], and any other law, rule, or regulation subject to the jurisdiction of the [SEC]," thus requiring a plaintiff asserting an anti-retaliation claim under Dodd-Frank to show either that the report was made to the Commission, or alternatively, that the report fell into one of the above four categories) (citation omitted), *with Asadi v. G.E. Energy (USA), L.L.C.*, 720 F.3d 620, 625 (5th Cir. 2013) (holding that the Dodd-Frank whistleblower protection provision created a private cause of action only for individuals who provide information relating to a violation of the securities laws to the SEC). The SEC, in its rules, took the same position as the *Egan* court. 17 C.F.R. § 240.21F-2(a) (2018), 17 C.F.R. § 249.1801 (2018); *see also Berman v. Neo@Ogilvy LLC*, 801 F.3d 145, 153 (2d Cir. 2015).

[47] *Somers v. Dig. Realty Tr.*, 850 F.3d 1045 (9th Cir. 2017), *rev'd*, 138 S. Ct. 767 (2018).

never knows if a whistleblower has in fact reported or will report to the SEC, and Sarbanes-Oxley as well as state law provide additional avenues for pursuing retaliation claims even absent an SEC report. Companies are thus well-advised to maintain robust lines of internal reporting and an appropriate system for following up on whistleblower complaints to enable internal resolution before a whistleblower feels compelled to report to the SEC or another federal or state regulator. Companies should strengthen the role of management in facilitating internal reporting, actively encourage employees to report anything they expect could raise a legal or ethical concern, and maintain multiple avenues for internal reporting, including an anonymous hotline for whistleblowing.

Moreover, irrespective of whether a whistleblower reports out to the SEC, the SEC's Division of Enforcement can be expected to scrutinize treatment of that individual and the company's internal response to the allegations as part of any government inquiry into the underlying conduct. Companies should therefore maintain robust anti-retaliation policies that emphasize that intimidation and retaliation against whistleblowers is strictly prohibited and ensure that senior management is well-trained and committed to compliance. Policies should explicitly state that nothing in the policy, or any other corporate policies, shall be construed to restrict employees from reporting to any governmental or regulatory agency. SEC staff may view retaliation, irrespective of whether actionable under Dodd-Frank, as evidence of bad intent.

Dodd-Frank also contains a bounty provision. The bounty provision incentivizes employees to go directly to the SEC, with concerns of violations, rather than first reporting such issues internally. SEC rules, however, urge individuals to report internally.[48] For example, the implementing regulations provide that a whistleblower who reports internally to the company and within 120 days reports the same information to the SEC could still be eligible to be considered a whistleblower under the statute.[49] Additionally, where the employee reports internally and then reports to the SEC, that employee will be eligible for the bounty as an original source of not only the information the employee provided, but also any information that the company

[48] 17 C.F.R. § 240.21F-4(b)(7) (2018).

[49] 17 C.F.R. § 240.21F-4(b)(7) (2018); 17 C.F.R. § 249.1801 (2018).

provides to the SEC, which could entitle the employee to a greater award.[50] The whistleblower's voluntary participation in an entity's internal compliance program is a factor that can increase the amount of the award.[51]

To be eligible for a bounty award, a whistleblower must: (a) voluntarily provide the Commission, (b) with original information, (c) that leads to the successful enforcement by the Commission of a federal court or administrative action, (d) in which the Commission obtains monetary sanctions totaling more than $1,000,000.[52]

Since the Commission issued its first award in 2012 through the end of Fiscal Year 2017, the Commission awarded approximately $160 million to 46 whistleblowers.[53] In Fiscal Year 2017, the Commission ordered whistleblower awards of nearly $50 million to 12 individuals, with three of those awards ranking in the Commission's ten largest awards issued to date.[54] This was the largest award issued under the program to date.[55]

U.S. Commodity Futures Trading Commission ("CFTC") Whistleblower Program

The CFTC rules also provide significant protections to whistleblowers. On May 22, 2017, the CFTC amended the rules governing its whistleblower program to significantly strengthen whistleblower protections against retaliation,[56] preclude reliance on confidentiality or arbitration clauses that would prevent employees from reporting to the CFTC, clarify that the CFTC itself may bring enforcement actions for violation of anti-retaliation rules (in addition to private enforcement), revise and clarify the whistleblower eligibility criteria,[57] and amend certain procedural aspects

[50] 17 C.F.R. § 240.21F-4(b)(7) (2018), 17 C.F.R. § 240; 17 C.F.R. § 2249.1801 (2018).

[51] *Id*.

[52] 17 C.F.R. § 240.21F-3(a) (2018).

[53] U.S. Sec. & Exch. Comm'n, *2017 Annual Report to Congress, Whistleblower Program*, at 1, 10, https://www.sec.gov/files/sec-2017-annual-report-whistleblower-program.pdf.

[54] *Id*. at 10.

[55] *Id*.

[56] 7 U.S.C. § 26(h)(1)(A) (2018).

[57] Notably, the amended rules (1) no longer require that a whistleblower be the "original source" of the information provided; (2) enable a whistleblower to qualify even if the whistleblower first reports a Commodities Exchange Act violation internally or to another authority, so long as a report is also made directly to the CFTC within 180 days; (3) enable a whistleblower to retain eligibility for an award based on information the whistleblower provided to foreign futures authorities before providing to the CFTC; (4) allow the CFTC to waive its procedural requirements upon a showing of "extraordinary circumstances," which are undefined, to provide added flexibility for whistleblowers of varying sophistication.

of the whistleblower program.[58] The CFTC's amendment aligns its regulations with existing SEC Rule 21F-17, and it is likely that it will be interpreted similarly.

PRACTICE TIP: BEST PRACTICES TO COMPLY WITH U.S. WHISTLEBLOWER REGULATIONS

- Strengthen the role of management in facilitating internal reporting.
  - For example, require management to take appropriate action to facilitate and promote compliance, hold management accountable for creating a retaliation-free environment, and require managers to report any issues brought to their attention through the appropriate channels.
- Encourage employees to report anything they expect could raise a legal or ethical concern.
- Maintain an anonymous hotline for employees to report potential concerns and ensure the hotline is well-publicized and easy to access.
- Maintain multiple avenues for internal reporting.
- Ensure the process for escalating concerns is transparent and a reasonable investigation of any whistleblower complaints is undertaken with prompt documentation of those efforts.
- Maintain a robust anti-retaliation policy and emphasize company policies and agreements that intimidation and retaliation against whistleblowers are strictly prohibited, even when the whistleblower's claims seem to lack merit.
- Ensure that senior management is well-trained and committed to compliance.
- Ensure that all internal reporting policies explicitly state that nothing in the policy, or any other corporate policies, shall be construed to restrict employees from reporting to any governmental or regulatory agency.

[58] For example, the existing Whistleblower Award Determination Panel (which was independent of the Division of Enforcement) is being replaced by a Claims Review Staff under the supervision of the Director of the Division of Enforcement and assisted by the Whistleblower Office staff, which it is hoped may provide a more direct route for whistleblower claims to translate into enforcement action.

Drafting Confidentiality and Non-Disclosure Agreements

Following a series of enforcement actions alleging that restrictive language in employment agreements violated Rule 21F-17, recent guidance from the SEC and other U.S. regulators, companies should heed the following best practices when drafting confidentiality and non-disclosure agreements to be signed by employees:

— State explicitly that nothing in any company policy or agreement is intended to restrict or prohibit reporting to government regulators or providing information in connection with a report or investigation.[59]

— Do not attempt to limit the types of information an employee may disclose to government regulators.[60]

— Make clear that current and former employees are not required to advise or seek permission from the company before disclosing information to a government regulator.[61]

— Do not attempt to limit current or former employees' ability to receive a monetary award from a government agency.[62]

---

[59] The SEC has stated that it is "reviewing, among other things, compliance manuals, codes of ethics, employment agreements, and severance agreements to determine whether provisions in those documents pertaining to confidentiality of information and reporting of possible securities law violations may raise concerns under Rule 21F-17." Office of Compliance Inspections and Examinations, *Examining Whistleblower Rule Compliance*, (Oct. 24, 2016) ("OCIE Guidance"). The SEC counsels against documents containing provisions that "purport to permit disclosures of confidential information only as required by law, without any exception for voluntary communications with the Commission concerning possible securities laws violations," meaning that such a provision is necessary but not sufficient in itself to notify employees of their whistleblower rights. *Id*. The SEC has also warned against policies that "require an employee to represent that he or she has not assisted in any investigation involving the [company]." *Id*. FINRA and the CFTC provide similar guidance. *See* FINRA Regulatory Notice 14-40 (2014); 17 C.F.R. § 165.19 (2018).

[60] The SEC has warned against provisions that "purport to limit the types of information that an employee may convey to the Commission or other authorities" or that "prohibit any and all disclosures of confidential information, without any exception for voluntary communications with the Commission concerning possible securities laws violations." OCIE Guidance.

[61] The SEC has warned against policies that "require an employee to notify and/or obtain consent from the [company] prior to disclosing confidential information, without any exception for voluntary communications with the Commission concerning possible securities laws violations." *Id*.

[62] The SEC counsels against documents containing provisions that "require departing employees to waive their rights to any individual monetary recovery in connection with reporting information to the government." *Id*. CFTC Rule 165 states that "[a] whistleblower retains eligibility for an award based on information provided by the whistleblower to certain specified persons or authorities . . . prior to the time that the whistleblower provided the information to the Commission." Commodity Futures Trading Comm'n, *Strengthening Anti-Retaliation Protections for Whistleblowers and Enhancing the Award Claims Review Process* (May 22, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/wbruleamend_factsheet052217.pdf.

— Ensure that company policies and agreements contain a clearly expressed anti-retaliation policy stating that employees cannot be punished or threatened with punishment in any way for whistleblower activity.[63]

— Ensure that company policies and agreements regarding confidentiality include a provision stating that as provided in 18 U.S.C. § 1833, employees will not be held criminally or civilly liable under any federal or state trade secret law for disclosure of a trade secret that is made: (1) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, in each case, solely for the purpose of reporting or investigating a suspected violation of law, or (2) in a complaint or other document filed in a lawsuit or proceeding, if such filings are made under seal.[64]

[63] Dodd-Frank provides a private cause of action for whistleblowers who suffer retaliation. Dodd-Frank Act, § 922(a); 15 U.S.C § 78u-6(h)(1)(A). The SEC and CFTC also have the authority to bring an action against an employer who retaliates against a whistleblower. *See* 17 C.F.R. § 240.21F-2(b)(2) (2018); 17 C.F.R. § 165.20 (2018).

[64] The Defend Trade Secrets Act of 2016, 18 U.S.C. § 1833 (2018).

CASE STUDY: NEARLY $15 MILLION AWARDED TO OUSTED GENERAL COUNSEL OF BIO-RAD LABORATORIES, INC. IN WHISTLEBLOWER RETALIATION ACTION

— Bio-Rad Laboratories, Inc.'s ("Bio-Rad") former general counsel sued the company under Sarbanes-Oxley, Dodd-Frank, and California state law, asserting that he was wrongfully terminated in retaliation for investigating and reporting to senior management potential violations of the Foreign Corrupt Practices Act in China. After a three-week trial, the jury awarded the ousted general counsel nearly $11 million in damages and punitive damages, and the parties stipulated to an additional $3.5 million owed to the former general counsel in costs and fees.[65]

Key Takeaways

— The *Wadler* court broadened the scope of potential liability for defendants under Sarbanes-Oxley and Dodd-Frank, finding that corporate directors of public companies can be held individually liable for retaliating against a whistleblower.[66] Absent the parties' agreement to dismiss all claims against individual defendants except Bio-Rad's CEO, other corporate directors could have been held liable.

— Privileged communications between a whistleblower and the company's directors, officers, in-house counsel, and even outside counsel, may be both discoverable and admissible in a whistleblower retaliation action to the extent the whistleblower reasonably believes the communications are necessary to prove his or her claims and defenses. This is particularly significant where the plaintiff is a former general counsel or in-house counsel of the company, positions that are ordinarily precluded from reporting to the SEC as a result of their ethical obligations to their clients, and typically viewed by employees and officers as confidential relationships in which to raise concerns and analyze solutions.[67]

Best Practices in the Wake of *Wadler*

— Ensure that indemnification agreements and D&O liability insurance cover whistleblower actions seeking individual accountability for officers and directors.

— Maintain timely and thorough personnel files, including by conducting regular performance evaluations with written documentation, and record negative performance issues as they occur. If a company decides to terminate an employee who previously voiced concerns of potential misconduct, it is critical that the company has a clear record demonstrating that the discipline is unrelated to the whistleblowing activity.

[65] Jury Verdict, *Wadler v. Bio-Rad Labs., Inc.*,141 F. Supp. 3d 1005 (N.D. Cal. February 7, 2017) (15-cv-02356-JCS), ECF No. 223.

[66] *Wadler v. Bio-Rad Labs., Inc.*, 141 F. Supp. 3d 1005, 1019, 1024 (N.D. Cal. 2015).

[67] *See id.*

U.K. Whistleblowing Regime

U.K. whistleblowing legislation protects a wide range of individuals including, among other things, employees, workers, and agency workers. The protections awarded to such individuals include the right not be subject to any detriment. Additionally, whistleblowers are regarded as being automatically unfairly dismissed if the reason or principle reason for the dismissal is that they blew the whistle.

In order to qualify for protection, a whistleblower must make a "qualifying disclosure" which is a "protected disclosure." A qualifying disclosure requires:

— There must be a disclosure of factual information, either verbally or in writing.

— The disclosure must show that one or more of the following types of wrongdoing has taken place, is taking place, or is likely to take place: (a) a criminal offense; (b) a breach of a legal obligation; (c) a miscarriage of justice; (d) danger to the health and safety of an individual; (e) damage to the environment; and/or (f) a deliberate concealment of information about any of the above.

— The whistleblower must subjectively believe that the wrongdoing has occurred, is occurring, or is likely to occur and his or her belief is objectively reasonable.

— The person making the disclosure must also have a reasonable belief that the disclosure is made in the public interest.[68]

To be protected, the disclosure must be made to specified categories of persons:

— **Internal disclosure:** A qualifying disclosure when made to a person's employer will be protected.

— **External disclosure to "prescribed persons":** A qualifying disclosure may be protected when it is made to "prescribed persons," which include, *inter*

[68] Public Interest Disclosure Act 1998 c. 23 (Eng.). The public interest condition relates only to disclosures made after June 25, 2013. For disclosures made before June 25, 2013, there is no public interest requirement but, instead, a good faith requirement applies.

alia, Her Majesty's Revenue and Customs, the Financial Conduct Authority, and the Prudential Regulation Authority. However, a qualifying disclosure to a prescribed person will only be protected where the whistleblower reasonably believes that the wrongdoing falls within the remit of the prescribed person and the information disclosed and allegation in it are substantially true.

— **Wider disclosure:** A qualifying disclosure made to the press may be protected in limited circumstances.

The U.K. whistleblower protections may be applied extraterritorially under certain conditions including where an employee travels often between offices in the United Kingdom and abroad and the employee's normal work base is in the United Kingdom, and where an employee shows a strong connection to the United Kingdom.[69]

Italian Whistleblower Protections

Italian Law No. 179/2017

Law No. 179/2017, which entered into force on December 29, 2017, requires companies that have adopted formal compliance programs pursuant to Legislative Decree No. 231/2001 ("Decree 231") also to implement a formal whistleblower program. Prior to Law No. 179/2017, only financial services and banking firms were required to implement formal whistleblower programs and protection against retaliation was limited to civil servants who reported the commission of wrongdoing.

A company may shield itself from liability if, among other things, prior to a crime's commission, the company adopts and effectively implements a compliance model designed to prevent crimes of the same kind as the one committed. Under Decree 231, companies are not required to adopt a compliance program, but they are encouraged to do so in order to avoid or at least minimize their liability in the event a crime is committed. Decree 231 sets forth certain requirements for compliance programs; for example, a compliance program must identify the activities that, when performed, may give rise to crimes or facilitate their commission; implement

[69] *See Serco Limited v. Lawson; Botham (FC) v Ministry of Defence; Crofts and others v. Veta Limited and others and one other action,* [2006] UKHL 3 (appeals taken from Eng. and Wales); *Ravat v. Halliburton Manufacturing and Services Ltd*, [2012] UKSC 1 (appeal taken from Scot.).

protocols governing the adoption and execution of decisions and the management of financial resources to prevent the commission of crimes; set forth reporting duties to the supervising body; and have a disciplinary code punishing noncompliance.[70]

Like Decree 231, Law No. 179/2017 does not require companies to adopt a compliance or whistleblower protection program; however, pursuant to the new paragraph 2-*bis* of Article 6, Decree 231, compliance programs shall include a whistleblowing procedure so that officers and employees can report violations of Decree 231. Accordingly, companies that have adopted compliance programs in accordance with Decree 231 should evaluate whether their policies comport with Law No. 179/2017, and companies seeking to implement compliance programs should incorporate whistleblower protections as part of those programs.

Under Law No. 179/2017, a compliance program must:

— Provide for more than one whistleblowing channel and be able to protect whistleblowers' identity, of which at least one has to be computerized.

— Prohibit acts of discrimination or retaliation against whistleblowers.

— Provide disciplinary measures for those who retaliate against a whistleblower and for the whistleblowers who intentionally or with gross negligence file false or unsubstantiated reports of violations.

— Provide formal whistleblower channels to directors, managers, and other subjects acting on behalf of the company or one of its organizational units, and persons subject to the direction or supervision of the above mentioned.

— Technically, a whistleblower program need not be available to self-employed contractors, external consultants, or others. However, as a practical matter, companies should nonetheless consider whether there are good reasons to include such persons within the scope of a whistleblower program.

[70] Article 6 ¶ 2, Decree 231.

— There is no requirement that anonymous whistleblower complaints be entertained, Law No. 179/2017 also requires that companies ensure the confidentiality of a whistleblower's identity to the extent permitted by Italian law.

Law No. 179/2017 also provides protection against retaliation by permitting whistleblowers to raise allegations of retaliatory and discriminatory acts arising from whistleblowing activities to the Senior Labor Inspectorate (*Ispettorato del Lavaro*) personally or through a labor union. In case of disputes concerning disciplinary measures, dismissals, transfers, or demotions imposed after the employee blew the whistle, Law No. 179/2017 provides that the burden of proof shifts, requiring the employer to demonstrate that the measure is based on grounds different from the reporting. The existence of strong anti-retaliation provisions means that companies should not only adopt their own anti-retaliation provisions, but also provide formal training to employees on those policies and to see that they are effectively enforced.

Italian Law No. 154/2014

As described above, the first law introducing whistleblowing procedures in the Italian private sector was Law No. 154/2014, which amended the Consolidated Finance Law (*Testo Unico della Finanza*) and the Consolidated Banking Law (*Testo Unico Bancario*) requiring banks and financial intermediaries to implement mechanisms to report breaches of financial and banking regulations.

Among other things, banks and financial intermediaries must provide:

— Specific and independent channels in order to allow their staff to report violations of banking and financial laws and regulations.

— Protection for employees who report breaches committed within the institution against retaliation, discrimination, or other types of unfair treatment.

— Protection of personal data concerning both the person who reports the breaches and the person who is allegedly responsible for a breach.

Compliance With Italian and European Privacy Law

In addition to the specific requirements of Law No. 179/2017 and predecessor legislation Law No. 154/2014 in the financial sector, whistleblowing procedures must also comply with Italian and European privacy law.

In July 2016, the European Data Protection Supervisor issued *Guidelines on processing personal information within a whistleblowing procedure*, listing detailed recommendations. These guidelines are an invaluable tool for any company wanting to implement a whistleblowing procedure compliant with data protection regulations. Specifically, companies should:

— Collect (and retain) only information which are relevant, adequate, and necessary for the investigation.

— Ensure the confidentiality of the information.

— Inform persons involved in the whistleblowing procedure about the processing of their data and provide such persons with a specific data protection statement as soon as practically possible. However, when this information can jeopardize the investigation, the disclosure can be deferred. Deferral of information should be decided on a case-by-case basis and the reasons for any restriction should be documented.

— Define proportionate conservation periods for the personal information processed within the scope of the whistleblowing procedure depending on the outcome of each case (a shorter retention period for reports that did not lead to an investigation).

— Implement both organizational and technical security measures based on a risk assessment analysis of the whistleblowing procedure, in order to guarantee a lawful and secure processing of personal information.

Companies should also consider how whistleblower allegations will be processed and what information will be provided to the whistleblower in view of the General

Data Protection Regulation ("GDPR").[71] Depending on the circumstances, and the nature of the information a whistleblower provides, the GDPR may limit the way in which whistleblower complaints can be processed.

German and French Whistleblower Protections

Germany and France do not have specific whistleblower protection laws in place. However, when whistleblowing programs imply the processing of personal data, they are subject to data privacy and protection regimes.[72]

Brazilian Whistleblower Protections

Brazil has no specific whistleblower protection in place. However, the Office of the Comptroller General ("CGU") has provided Corporate Integrity Guidelines for Private Companies ("CGU Guidelines") that relate to whistleblower procedures in connection with building strong anti-corruption policies.

The CGU Guidelines were issued to clarify certain anti-corruption measures (the "Integrity Program") emphasized by Law No. 12,846/2013, known as the Anti-Corruption Law or Clean Companies Act, under which a company's adoption of the Integrity Program can be recognized as a mitigating factor for malpractice. Law No. 12,846/2013 establishes that legal entities in Brazil are subject to strict administrative and civil liabilities for offences they commit either in their interest or to their benefit against national and foreign public officials.

The Integrity Program under Law No. 12,846/2013 focuses on equipping companies with anti-corruption measures aimed at preventing, detecting, and providing remedies for harmful acts committed against national and foreign public administrations. Companies with existing compliance programs, i.e. those that have a framework of policies and rules set forth to ensure a company is abiding by government laws and regulations, should work to incorporate anti-corruption measures into their existing programs. In connection with those programs, companies should prepare or revise their code of ethics and conduct, as well as the rules, policies, and procedures to prevent irregularities; develop detection mechanisms or channels for reporting irregularities (alerts or red flags, reporting channels, and mechanisms aimed at

[71] *See* Chapter V: Data Privacy & Blocking Statutes.

[72] *See* Chapter V: Data Privacy & Blocking Statutes.

protecting whistleblowers); and define disciplinary measures in cases of violations and remediation measures.

The CGU Guidelines state that a company with a well-structured Integrity Program should have whistleblowing channels for receiving complaints. Specifically, companies should:

— Evaluate the need to adopt several means for receiving complaints, such as suggestion boxes, a hotline, through the internet, and alternatives to online reporting.

— Establish policies to ensure the protection of the whistleblower, such as the possibility of receiving anonymous complaints and the prohibition to retaliate against whistleblowers.

— Establish confidentiality rules to protect whistleblowers who do not want to be known publicly.

— Provide means for the whistleblower to track the progress of his or her complaint.

— Provide training to senior managers regarding the whistleblower program and procedures.

— Explain the existence and use of whistleblowing channels to employees through the company's code of ethics or conduct, and inform employees that retaliation for whistleblowing is prohibited.[73]

[73] *See* Office of the Comptroller General – CGU, *Corporate Integrity Guidelines for Private Companies* (Sep. 2015).

Employment-based Protections

What Can an Employer Do With Employee Communications?

In the United States, employers regularly monitor employees' work communications. Employment at will governs in all states except Montana, and employees generally consent to monitoring by their employers by signing the company's technology policy, which gives the company ownership over the communications and/or authorization to monitor communications.

Even federal privacy statutes, such as the Electronic Communications Privacy Act ("ECPA"), have explicit exceptions that allow for monitoring.[74] ECPA has a consent exception such that if an employer is a party to or has the consent of a party to the communications, there is no violation of the act.[75] Knowing consent destroys any reasonable expectation of privacy. ECPA also has an "ordinary course of business" exception allowing companies to monitor business-related calls and communications.[76] Lastly, ECPA has a "provider" exception under which an employer who supplies the system being monitored is a "provider" and may monitor the communications.[77]

In Europe, the GDPR governs data protection and privacy for all individuals within the EU and addresses the export of personal data outside the EU.[78]

What To Do When Employees, Whether Current or Former, Invoke Their Fifth Amendment Rights

Although whistleblowers are protected by state and federal whistleblower laws against retaliatory discharge for blowing the whistle, there is generally no protection for an employee who refuses to assist in an internal investigation by exercising his or her Fifth Amendment right against self-incrimination. Two employees of Marsh

[74] 18 U.S.C. § 2510 *et seq.* (2018).

[75] *See* 18 U.S.C. § 2511(2)(d) (2018).

[76] *See* 18 U.S.C. §§ 2510(5)(a); 2511(2)(a)(i) (2018).

[77] *See, e.g., Fraser v. Nationwide Mut. Ins*, 352 F.3d 107, 114-15 (3d Cir. 2003) (holding that employer-operated email system was excepted from Title II of the ECPA).

[78] For further detail on the GDPR, *see* Chapter V: Data Privacy & Blocking Statutes.

& McLennan, an international insurance broker-dealer, faced this issue in *Gilman v. Marsh & McLennan Companies, Inc.*[79] In that case, the Second Circuit held that the insurance broker-dealer's demands that its employees sit for interviews regarding their participation in an alleged criminal bid-rigging scheme was not a state action that infringed on the employees' Fifth Amendment right against self-incrimination. Thus, the broker-dealer was not precluded from firing the employees for cause and denying them severance pay, and the Second Circuit held that the broker-dealer had "good institutional reasons" for requiring the employees to sit for interviews or lose their jobs. The Second Circuit noted "a company is not prohibited from cooperating, and typically has supremely reasonable, independent interests for conducting an internal investigation and for cooperating with a governmental investigation, even when employees suspected of crime end up jettisoned. A rule that deems all such companies to be government actors would be incompatible with corporate governance and modern regulation."[80]

[79] *Gilman v. Marsh & McLennan Companies, Inc.*, 826 F.3d 69, 76 (2d Cir. 2016).

[80] *Id.*

Chapter VII:
Cooperation

Summary

Cooperation:

— Requires voluntary and affirmative assistance beyond merely responding to compulsory requests for information.

— Involves providing information relevant to the investigating authority's inquiry.

— Generally does not require a party to waive privilege.

— May require assisting authorities in building cases against individuals.

— Will generally be considered in tandem with other factors (such as, for example, severity of the conduct) when determining what, if any, credit is warranted for cooperation.

Cooperation Credit:

— Depending on the facts, may take the form of a:

- Deferred prosecution agreement ("DPA");
- Non-prosecution agreement ("NPA");
- Cooperation agreement;
- Reduction in fines or other penalties, or the imposition of remedial measures;
- Reduction in jail time (for culpable individuals); or
- Declination of enforcement action.

Introduction

Cooperation in the context of a government investigation or enforcement action means voluntarily providing affirmative assistance to the investigating authority in the authority's investigation of a crime or violation that goes beyond what is legally required.[1] Regulatory and law enforcement authorities offer incentives to companies that cooperate in their investigations and enforcement actions, including lower penalties or fines, or declination of prosecution altogether. Consequently, while it comes with risks and costs, cooperation can also be a valuable tool for corporations looking to reduce their liability exposure. However, the costs and risks of cooperation can at times be significant and must be considered before a decision is made whether to cooperate. Investigating authorities are known frequently to quote the adage that you cannot cooperate halfway. For similar reasons, once a company has started to cooperate, it is frequently ill-advised to stop cooperating. Moreover, because the notion of cooperation can be subjective and investigating authorities retain substantial discretion with respect to the type and extent of cooperation credit to extend, it is difficult to have a concrete sense of the actual benefits of cooperation prior to the conclusion of an investigation—and even then the tangible benefits may be uncertain. This chapter explores some relevant considerations in determining whether and how to cooperate in an investigation, as well as available guidance from different authorities as examples of the factors considered and cooperation credit extended (or denied) in different contexts.

What Is Cooperation?

The exact manner in which cooperation is defined in the context of an investigation has both objective and subjective components and may be case and agency specific. Different authorities vary in the factors considered and credit awarded, which may further also depend on the particular circumstances of a given case. There are, however, general factors that are typically considered by authorities, which can be instructive in formulating a cooperation strategy.

[1] *See, e.g., Frequently Asked Questions: Corporate Cooperation and the Individual Accountability Policy*, Dep't of Just., (Nov. 30, 2016), https://www.justice.gov/file/913911/download.

PRACTICE TIP:
FACTORS TYPICALLY CONSIDERED IN DETERMINING THE EXTENT OF COOPERATION

- The timeliness of the cooperation, including whether the company self-reported any actual or potential misconduct.
- How quickly misconduct was detected, escalated, and addressed.
- The quality of the company's compliance and reporting program, and whether any deficiencies were resolved.
- The quality of the internal investigation, including whether the company provided information about culpable individuals as well as information that the investigating authority may not have been able to obtain on its own.
- The quality of practical assistance offered to the investigating authority, including whether documents were produced and witnesses were made available in a timely manner.
- Other remediation efforts undertaken after the wrongdoing was discovered.
- Resources devoted by the company to cooperation and correspondingly resources conserved as a result of the cooperation, and the degree to which the information provided otherwise furthered the investigation.

Practically Speaking, What Does Cooperation Look Like?

Many government and regulatory authorities award cooperation credit for a company's affirmative assistance with an investigation. A company should anticipate that different authorities vary in their willingness to articulate the precise metrics they apply in assessing cooperation, including how they calculate any cooperation credit and the amount of credit that they will award.

Cooperation in the United States

In the United States, government authorities—including, for example, the Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC" or "Commission")—typically consider a host of factors in determining cooperation credit. These factors range from assisting with relatively prosaic but costly tasks, such as translations, to providing the government with evidence,

often located abroad, that it may not have been able to obtain without company cooperation. In general, authorities are willing to provide the most credit—including declining to bring a case at all—to entities that had low levels of culpability, but nonetheless provided extensive assistance, including in providing timely factual information that can be used to build cases against culpable individuals.

The DOJ

The DOJ, for example, has—at least for certain types of misconduct—been willing to articulate how it quantifies cooperation credit with significant granularity.

DOJ'S FOREIGN CORRUPT PRACTICES ACT (FCPA) CORPORATE ENFORCEMENT POLICY

In November 2017, the DOJ implemented the Foreign Corrupt Practices Act ("FCPA") Corporate Enforcement Policy.[2] This policy built on an earlier pilot program, adopted by the Fraud Section of the DOJ in April 2016, which articulated a written framework of penalty reductions to motivate companies "to voluntarily self-disclose FCPA-related misconduct."[3] Under the Corporate Enforcement Policy, a company may qualify for cooperation credit if it pays all "disgorgement, forfeiture, and/or restitution resulting from the misconduct at issue,"[4] and meets the requirements set forth below:

Voluntary self-disclosure[5]

— Disclose wrongdoing "prior to an imminent threat of disclosure or government investigation."

— Disclose "within a reasonably prompt time of becoming aware of the offense."

— Disclose "all relevant facts known to the company, including all relevant facts about individuals involved in the violation."

[2] *See* Dep't of Just., *U.S. Attorneys' Manual* 9-47.120 (Nov. 1997) ("USAM").

[3] *See The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance*, Criminal Div., Dep't of Just. (Apr. 5, 2016), https://www.justice.gov/archives/opa/blog-entry/file/838386/download. The pilot program was originally set to expire in April of 2017, but was instead allowed to continue in full force until the DOJ completed an evaluation of the program. Jonathan Sack, *DOJ Announces It Will Extend FCPA "Pilot Program*," Forbes (Mar. 13, 2017), https://www.forbes.com/sites/insider/2017/03/13/doj-announces-it-will-extend-fcpa-pilot-program/#440722a51d3e.

[4] USAM § 9-47.120(1).

[5] *Id*. § 9-47.120(3)(a).

Full cooperation[6]

— Disclose, on a timely basis, all facts relevant to the wrongdoing at issue, including facts concerning the involvement of officers, employees, or agents.

— Engage in proactive, rather than reactive, cooperation, including disclosing relevant facts even when not asked to do so and identifying opportunities for the government to obtain relevant evidence not in the company's possession and unknown to the government.

— Preserve, collect, and disclose relevant documents and information relating to their provenance, including foreign and third-party documents and, where requested, document translations.

— Where requested, "de-conflict" an internal investigation with the government investigation.

— Make company personnel, including individuals located outside of the United States, available for DOJ interview upon request.

— Disclose all overseas documents, except where foreign law prohibits disclosure (with the responding party bearing "the burden of establishing the prohibition").

Remediation[7]

— Thoroughly analyze the root causes underlying the identified conduct and implement remedial steps to address the causes identified.

— Implement an effective compliance and ethics program based on specified criteria.

— Appropriately discipline culpable employees.

— Demonstrate appropriate retention of business records, including prohibiting improper destruction or deletion.

— Implement measures to reduce the risk of repetition of the misconduct identified.

[6] *Id*. § 9-47.120(3)(b).

[7] *See id*. § 9-47.120(3)(c).

The Corporate Enforcement Policy offers a rare degree of transparency as to the cooperation credit available to companies meeting the above requirements. Specifically, where a company has paid all required disgorgement or restitution, and has voluntarily self-disclosed, fully cooperated, and timely remediated:

— It is presumptively entitled to a declination so long as there are no "aggravating circumstances involving the seriousness of the offense or the nature of the offender."

— Where a criminal resolution is warranted, the DOJ will accord, or recommend to a sentencing court, a 50% reduction off of the low end of the U.S. Sentencing Guidelines (U.S.S.G.) fine range, except in the case of a recidivist.

— The DOJ generally will not appoint a monitor, so long as the company has implemented an effective compliance program at the time of the resolution.[8]

Additionally, if a company does not voluntarily disclose the wrongdoing, but later cooperates and fully remediates, "limited credit" may be available, whereby the company will receive, or DOJ will recommend to a sentencing court, "up to a 25% reduction off of the low end of the U.S.S.G. fine range."[9]

In a sign that the DOJ views the Corporate Enforcement Policy to be a successful model for promoting self-disclosure and cooperation, it has announced that the Corporate Enforcement Policy will serve as nonbinding guidance for non-corruption criminal cases investigated by the DOJ in the future.[10]

[8] *Id*. § 9-47.120(1).

[9] *Id*. § 9-47.120(2).

[10] *See generally*, Jonathan Kolodner et al., *DOJ Announces Expansion of Approach Encouraging Self Reporting and Cooperation*, Cleary Enforcement Watch (Mar. 5, 2018), https://www.clearyenforcementwatch.com/2018/03/doj-announces-expansion-approach-encouraging-self-reporting-cooperation/.

DOJ ANTITRUST DIVISION LENIENCY PROGRAM

Since 1993, the DOJ's Antitrust Division (the "Division") has offered a formal leniency program designed to facilitate cooperation in antitrust investigations.[11] Two types of leniency are available:[12]

— **Type A Leniency:** Automatically available where the Division was not aware of the anti-competitive activity from any other source prior to the company's reporting, *and* the company:

- Promptly and effectively terminates its participation in the misconduct upon discovery.
- Reports the wrongdoing with candor and completeness.
- Provides full, continuing, and complete cooperation to the Division throughout the investigation.
- Confesses to wrongdoing as a corporate act.
- Pays restitution where possible.
- Was not the ringleader of the conspiracy and did not coerce any participation in the conspiracy.

— **Type B Leniency:** Available where the Division has already received information about the illegal antitrust activity at the time of the application, regardless of whether an investigation has commenced, *and*:

- The company meets the other requirements for Type A Leniency.
- The Division has not yet obtained evidence against the company that is likely to result in a sustainable conviction.
- The granting of leniency would not be unfair to others given the factors relating to the company's participation.

[11] *See Corporate Leniency Policy*, Dep't of Just. (Aug. 10, 1993), https://www.justice.gov/atr/file/810281/download.

[12] *See Frequently Asked Questions about the Antitrust Division's Leniency Program and Model Leniency Letters*, Dep't of Just. (Jan. 17, 2017), https://www.justice.gov/atr/page/file/926521/download.

- The company is the first "to come forward and qualify for leniency with respect to the illegal activity being reported."[13]

Successful corporate leniency applicants may obtain substantial benefits,[14] including:

— Avoidance of all criminal penalties, which can amount to tens or hundreds of millions of dollars in a typical antitrust case.[15]

— For antitrust crimes, protection from criminal prosecution and possible incarceration for the company's officers and directors.[16]

Moreover, even if a company is unsuccessful in its leniency application, under the Division's "Leniency Plus" policy, an unsuccessful leniency applicant for a particular conspiracy may qualify for leniency in other markets in which it competes.[17]

As a practical matter, regardless of whether a governmental authority enumerates the specific actions it expects cooperating companies to undertake or only sets forth broader cooperation principles, investigating agencies typically expect cooperation to involve many, if not all, of the enumerated actions set forth in the DOJ's FCPA Corporate Enforcement Policy above, and it can, therefore, serve as a helpful reference in cooperating with other authorities as well. Further, while the DOJ has provided some quantification with respect to the cooperation credit available under its FCPA policy and Antitrust Leniency Program, each case differs and the

[13] *Id*. at 5. The Division will only award leniency to the first qualifying corporation for a particular antitrust conspiracy. Due to this "first-in-the-door" policy, companies have an incentive to make a leniency application as soon as they become aware of misconduct, before any co-conspirators or employees do so. *Id*. at 5–6. Accordingly, the Division has adopted a policy that allows a company to secure its place at the front of the line by putting down a "marker." To obtain a marker, a company's counsel must typically: "(1) [R]eport that he or she has uncovered some information or evidence indicating that his or her client has engaged in a criminal antitrust violation; (2) disclose the general nature of the conduct discovered; (3) identify the industry, product, or service involved in terms that are specific enough to allow the Division to determine whether leniency is still available and to protect the marker for the applicant; and (4) identify the client." *Id*. at 2-3. The corporate applicant thereafter has a finite period of time (generally 30 days) to perfect the leniency application. *Id*. at 4.

[14] *See id*. at 4-5.

[15] Scott D. Hammond, Dir. of Criminal Enforcement, Dep't of Just., *Fifteenth Annual Institute on White Collar Crime, When Calculating The Costs And Benefits Of Applying For Corporate Amnesty, How Do You Put A Price Tag On An Individual's Freedom?* (Mar. 8, 2001), https://www.justice.gov/atr/speech/when-calculating-costs-and-benefits-applying-corporate-amnesty-how-do-you-put-price-tag.

[16] If a company qualifies for Type A Leniency, "all current directors, officers, and employees of the corporation who admit their involvement in the criminal antitrust activity as part of the corporate confession . . . and continue to assist the Division throughout the investigation" will receive leniency. *Frequently Asked Questions about the Antitrust Division's Leniency Program and Model Leniency Letters* 20, Dep't of Just. (Jan. 26, 2017), https://www.justice.gov/atr/page/file/926521/download (last visited Aug. 3, 2018). If a corporation qualifies for Type B Leniency, the Division has greater discretion with respect to the charging decision. *Id*. However, "individuals who come forward with the corporation will still be considered for immunity from criminal prosecution" as if they had approached the Division on an individual basis. *Id*. at 20–21.

[17] *See id*. at 9–11. Note, however, that under the corresponding "Penalty Plus" policy, if a company applies for leniency due to one criminal violation, but fails to report an additional violation that the Division discovers, the leniency application is voided, and the Division will likely seek a more severe punishment for the additional crime. *See id*. at 11–12.

precise amount of cooperation credit assigned is ultimately within the discretion of the government attorneys investigating the case. Thus, companies should keep in mind that while cooperation may garner real benefits, other factors—such as the size and scope of any misconduct or the amount of publicity it garners—may also shape the contours of any resolution.

Other Investigative Agencies

In contrast to the detailed frameworks set forth in the DOJ's FCPA Corporate Enforcement Policy and Antitrust Leniency Program, other agencies—for example, the SEC and the Commodity Futures Trading Commission ("CFTC")—eschew detailed descriptions of concrete steps necessary to garner cooperation credit, much less undertake to quantify such credit. Instead, these agencies set out a series of principles that the agency looks to in determining whether an entity cooperated with an investigation.

THE SEC'S COOPERATION PROGRAM

The SEC has articulated four factors identified in the "Seaboard Report," which sets forth a framework for evaluating cooperation by companies.[18] These factors are:

— **Self-policing** prior to the discovery of the misconduct, including having effective compliance procedures in place and an appropriate tone at the top.

— **Self-reporting** misconduct when it is discovered, including conducting a thorough review of the nature, extent, origins, and consequences of the misconduct, and promptly and completely disclosing the misconduct to regulatory agencies, to self-regulatory organizations, and to the public.

— **Remediation** including dismissing or appropriately disciplining wrongdoers, modifying and improving internal controls and procedures to prevent recurrence of the misconduct, and appropriately compensating those negatively affected by the misconduct.

— **Cooperation** with law enforcement authorities, including providing SEC staff with all information relevant to the underlying violations and the company's remedial efforts.

In weighing the Seaboard factors, the SEC retains broad discretion to evaluate each case individually. Additionally, the SEC may also take into account other factors, including:

— The nature of the misconduct, including how it arose, and the company's culture and compliance procedures.

— Where in the organization the misconduct arose and what that indicates about the way the entity does business.

— The duration of the misconduct.

— The extent of the harm, how it was detected, and what steps the company took following detection.[19]

[18] *See* Sec. Exch. Comm'n, Enforcement Manual § 6.1.2 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

[19] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions Decisions*, Exch. Act Release No. 44969 (Oct. 23, 2001), https://www.sec.gov/litigation/investreport/34-44969.htm.

THE CFTC'S ADVISORIES ON COOPERATION AND SELF REPORTING

In September 2017, the CFTC Enforcement Division issued an "Updated Advisory on Self Reporting and Full Cooperation,"[20] which updates two prior advisories issued in January of that year,[21] in an effort to provide "greater transparency about what the [CFTC] requires from companies and individuals seeking mitigation credit for voluntarily self-reporting misconduct, fully cooperating with an investigation, and remediating[.]"[22]

In the January advisory addressing cooperation by companies, the CFTC indicated that it required more than just "ordinary cooperation or mere compliance" with law.[23] Rather, the CFTC considers the following factors in evaluating cooperation:

— *The value of cooperation to the CFTC's investigation or enforcement action*, including the timeliness of the disclosure.

— *The value of the company's cooperation in connection with the CFTC's broader enforcement interests*, including conservation of enforcement resources.

— *The relative culpability of the cooperating company*, including the circumstances of the misconduct, the company's history, and remediation.[24]

Under the January guidance, cooperation credit was discretionary, and could "range from the Division recommending no enforcement action" to "reduced charges or sanctions."[25]

The guidelines issued in September 2017 clarify the credit a company can expect for cooperation. Namely, where a company: (i) voluntarily self-discloses misconduct, (ii) fully cooperates, and (iii) appropriately remediates, the CFTC Enforcement Division

[20] *See Enforcement Advisory: Updated Advisory on Self-Reporting and Full Cooperation*, Commodity Futures Trading Comm'n (Sep. 25, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryselfreporting0917.pdf.

[21] *See Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies*, Commodity Futures Trading Comm'n (Jan. 19, 2017), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf; *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Individuals* [hereinafter Recommendations for Individuals], Commodity Futures Trading Comm'n (Jan. 19, 2017), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryindividuals011917.pdf.

[22] *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies*, Commodity Futures Trading Comm'n (Sept. 25, 2017), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryselfreporting0917.pdf.

[23] *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies* at 1, Commodity Futures Trading Comm'n (Jan. 19, 2017) https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf.

[24] *Id*. at 1, 4–5.

[25] *Id*. at 1–2.

"will recommend that the Commission consider a substantial reduction" in penalty and may, in extraordinary circumstances, recommend a declination of prosecution.[26]

— The voluntary disclosure requirement is satisfied where the company:

  - Discloses the misconduct before there is "imminent threat" of exposure.
  - Discloses within a "reasonably prompt" time after learning of the misconduct.
  - Includes all relevant facts known to the company at the time of the disclosure, including facts about relevant individuals involved.

While the CFTC makes clear that the most substantial reductions are reserved for companies that self-report, reductions in penalties are also available even if a company does not voluntarily disclose wrongdoing, but later fully cooperates and remediates.[27]

PRACTICE TIP:
COMPANIES SEEKING THE MAXIMUM BENEFITS FROM COOPERATION SHOULD, AT A MINIMUM, ANTICIPATE

— Affirmatively self-disclosing information from an internal investigation prior to the government knowing of or investigating the conduct.

— Quickly preserving, collecting, and disclosing all relevant documents, including all relevant documents located outside of the United States to the extent permitted by law (and asserting any legal barriers to doing so).[28]

— Providing translations of foreign-language documents.

— Identifying opportunities for the government to obtain relevant evidence unknown to government or beyond the reach of its investigative authority.

— Making officers or employees available to the government for interview, including those in foreign jurisdictions.

— Agreeing to continue cooperating in an investigation.

[26] *Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies* at 2, Commodity Futures Trading (Sept. 25, 2017) http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryselfreporting0917.pdf.

[27] *Id*. at 2–3.

[28] Cross-border data issues, such as data privacy and blocking statutes, are discussed in further detail in Chapter V: Data Privacy & Blocking Statutes.

Cooperation Outside of the United States

In jurisdictions outside of the U.S., law enforcement and regulatory authorities may offer credit for cooperation, and similar competing considerations may impact a company's decision regarding whether to cooperate.

United Kingdom

In the United Kingdom, the Serious Fraud Office ("SFO"), which investigates and prosecutes "serious or complex fraud, bribery and corruption,"[29] and the Financial Conduct Authority ("FCA"), which regulates financial services firms,[30] each adopt certain measures and practices (including those which provide the possibility for reduced penalties) intended to incentivize corporations to cooperate with their investigations. In particular, a material incentive to cooperate with the SFO was provided to companies through the introduction of a DPA regime in February 2014.

By way of illustration, the SFO has published its "Guidance on Corporate Prosecutions" which clarifies that a "genuinely proactive approach adopted by [a company's] management team" will be a factor which militates against a criminal prosecution.[31] While the SFO does not expressly define what constitutes a "genuinely proactive approach" to cooperation, its Guidance on Corporate Prosecutions, Deferred Prosecution Agreement Code of Practice, and case law relating to the (relatively few) awards of DPAs to date[32] indicate relevant factors that the SFO might take into account in assessing the level of a company's cooperation.

[29] *See About Us*, Serious Fraud Office, https://www.sfo.gov.uk/about-us/ (last visited Aug. 3, 2018).

[30] *See About the FCA*, Fin. Conduct Auth., https://www.fca.org.uk/about/the-fca (last visited Aug. 3, 2018).

[31] *See Guidance on Corporate Prosecutions* ¶ 32, Serious Fraud Office, https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/corporate-self-reporting/ (hereinafter Guidance on Corporate Prosecutions); *Deferred Prosecution Agreements Code of Practice* ¶ 2.8.2(i) (hereinafter Deferred Prosecution Agreements Code of Practice), Serious Fraud Office, https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/.

[32] In contrast to the United States, the decision by the SFO to enter into DPA negotiations, and the terms of a proposed DPA, are both subject to the approval of the English courts. *See* Crime & Courts Act 2013, Sched. 17 ¶¶ 7–8, http://www.legislation.gov.uk/ukpga/2013/22/schedule/17/enacted.

SFO INVESTIGATIONS: FEATURES OF GOOD COOPERATION

In the context of SFO investigations, elements of good cooperation may include:

— **Voluntary Self-Reporting of Misconduct:** Self-reporting of misconduct is indicated as a factor that weighs against prosecution[33] and may weigh in favor of a DPA.[34] In assessing the effectiveness of a company's self-reporting, prosecutors may consider the following:

- How early the company self-reported after becoming aware of wrongdoing.
- The extent to which the company involved the prosecutor in the early stages of an investigation (for example, to discuss work plans, timetables, "or to provide the opportunity for the prosecutor to . . . commence an early criminal investigation").
- Whether the company identified all relevant information, including culpable individuals.[35]

— **Identifying Witnesses and Facilitating Interviews:** Proactive cooperation will typically involve identifying relevant witnesses and making them available for interview.[36] Moreover, a company will usually be expected to disclose witness accounts to the SFO, as well as the documents shown to witnesses.[37]

— **Disclosing Internal Investigation Documents:** In addition to providing the SFO with documents shown to witnesses, a cooperating company should expect to share documents relating to any internal investigation of the misconduct that it may have conducted,[38] which may include investigation interview summaries or memoranda.[39]

---

[33] *See Guidance on Corporate Prosecutions* ¶ 32. By contrast, the "[f]ailure to report wrongdoing within reasonable time " and the "[f]ailure to report properly and fully the true extent of the wrongdoing" are both factors that weigh in favor of the SFO commencing prosecution. *Id.* at 7–8.

[34] *See* Deferred Prosecution Agreements Code of Practice ¶ 2.9.1. *See also Serious Fraud Office v. Standard Bank PLC* [2015] EWHC (QB) at 30(Eng.); *Serious Fraud Office v. XYZ Ltd.* [2016] EWHC (QB) at 57 (Eng.).

[35] Deferred Prosecution Agreements Code of Practice ¶¶ 2.9.1–2.9.2.

[36] *See, e.g.*, *Serious Fraud Office v. Standard Bank PLC* [2015] EWHC (QB) at 30 (Eng.) The U.K. authorities have recently adopted an increasingly proactive approach to challenging claims of legal privilege made by corporations over investigation materials, including notes of interviews with witnesses. In this regard, recent decisions of the English courts have significantly limited the circumstances in which privilege claims may be made over notes of interviews with witnesses. *See supra* Chapter IV: Preserving Legal Privilege.

[37] Deferred Prosecution Agreements Code of Practice ¶ 2.8.2(i). In certain instances, a company may demonstrate proactive compliance by deferring its internal interviews until the SFO has had the opportunity to complete its own interviews. *Serious Fraud Office v. Rolls Royce* [2017] EWHC (QB) ¶ 20(ii) (Eng.).

[38] Deferred Prosecution Agreements Code of Practice ¶ 2.8.2(i).

[39] *Serious Fraud Office v. Standard Bank PLC* [2015] EWHC (QB) at 30 (Eng.); *Serious Fraud Office v. XYZ Ltd.* [2016] EWHC (QB) at 30 (Eng.); *Serious Fraud Office v. Rolls Royce* [2017] EWHC (QB) ¶ 20(ii) (Eng.). While the SFO has previously allowed companies to provide either summaries of interviews or interview memoranda (on the basis of a limited privilege waiver), the English courts have recently taken a strict approach to claims of privilege over internal interview memoranda. *See supra* Chapter IV: Preserving Legal Privilege. As a result, it is not clear that the SFO will necessarily allow companies to provide internal interview memoranda on the basis of a limited privilege waiver in the future, which may have important implications for privilege waivers in the United States.

— **Providing Timely and Complete Responses to SFO Information Requests:** A cooperating company should voluntarily provide material responsive to SFOs requests.[40] In addition to providing the SFO with all relevant hard copy documents, further cooperation credit has been extended to companies that have provided the SFO with direct access to their electronic document review platform.[41]

— **Waiving the right to filter responsive material for privilege:** In at least one instance to date, a company's decision to waive the right to filter and review its documents for privilege, and instead allow its materials to be reviewed for privilege by independent counsel, was viewed as a factor that weighed in favor of allowing the company to enter into a DPA.[42]

In addition to the foregoing, the SFO may consider other factors, including, for example: remedial actions taken by the company, such as compensating victims;[43] agreeing to ongoing cooperation with domestic and overseas authorities;[44] and consulting the SFO with respect to responding to media coverage.[45]

The FCA has similarly articulated its expectations on cooperation, through its Principles for Business and the FCA Handbook. The FCA's Principles for Businesses are mandatory and binding on FCA-regulated firms, and Principal 11 provides that "[a] firm must deal with its regulators in an open and cooperative way, and must disclose to the [regulator] appropriately anything relating to the firm of which that regulator would reasonably expect notice."[46] Where a company's internal investigation triggers the notice requirement of Principle 11, the firm should discuss the scope of its investigation with the FCA as early as possible. Although the FCA has previously made clear that it will not rely on a company's internal investigation in place of its own, it may consider the company's findings in assessing its cooperation.[47]

---

[40] *Serious Fraud Office v. Standard Bank PLC* [2015] EWHC (QB) at 52 (Eng.); *Serious Fraud Office v. XYZ Ltd.* [2016] EWHC (QB) at 26, 54 (Eng.).; *Serious Fraud Office v. Rolls Royce* [2017] EWHC (QB) ¶ 20(iii) (Eng.).

[41] *Serious Fraud Office v. Rolls Royce* [2017] EWHC (QB) ¶¶ 19-20 (Eng.).

[42] *Id.*

[43] Guidance on Corporate Prosecutions ¶ 32; Deferred Prosecution Agreements Code of Practice 2.8.2(i).

[44] *Serious Fraud Office v. Standard Bank PLC* [2015] EWHC (QB) at 30.

[45] *Serious Fraud Office v. Rolls Royce* [2017] EWHC (QB) ¶ 20 (Eng.). In this respect, Rolls Royce effectively relinquished control over the investigation by responding to media and governmental inquiries in a manner agreed upon with the SFO. *Id.* ¶¶ 20, 122.

[46] *Handbook on Rules and Guidance*, Fin. Conduct Auth., PRIN 2.1.1(11), https://www.handbook.fca.org.uk/handbook/PRIN.pdf.

[47] Jamie Symington, Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), Fin. Conduct Auth., Pinsent Masons Regulatory Conference, *Internal Investigations by Firms* (Nov. 5, 2015), https://www.fca.org.uk/news/speeches/internal-investigations-firms (explaining that a company's own investigation can be "immensely helpful" to the FCA in resolving investigations efficiently, but the investigation must be conducted transparently and all relevant underlying evidence should be provided to the FCA so that it can conduct its own factual analysis).

Similarly, under the FCA Handbook, maintaining an open and cooperative relationship between the company and FCA supervisors may, in some cases, lead the FCA to decide not to carry out a formal investigation, and to instead allow the company to take the "necessary remedial action agreed with its supervisors to deal with the FCA's concerns."[48]

THE FCA'S GUIDANCE FOR COOPERATING COMPANIES: FACTORS CONSIDERED

Principle 11's requirement to disclose any information of which the FCA would reasonably expect notice, includes:

— Notifying the FCA within a reasonable time period of any significant failure of the company's systems or controls, as well as any action which a company proposes to take which would result in a material change in its capital adequacy or solvency.[49]

— Immediately notifying the FCA if the company becomes aware of significant fraud, "irregularities in its accounting or other records," serious misconduct by one of its employees,[50] or any significant violation of competition law.[51]

In addition, the FCA Handbook notes factors that are relevant to the FCA's assessment of a company's cooperation, including:

— **The Company's Overall Relationship with the FCA:** The FCA is less likely to use enforcement tools if a firm has a strong track record of open communication with the FCA, and has otherwise demonstrated that senior management takes compliance seriously. Against a background of ongoing cooperation, the FCA may conclude that the use of enforcement tools is not necessary to further the FCA's aims and objectives.[52]

— **The Company's Response to Particular Instances of Misconduct:** The FCA will also consider how the company responded to the particular misconduct under investigation, including whether the company self-reported; the extent to which the

[48] *Handbook on Rules and Guidance*, Fin. Conduct Auth., Enforcement Guide 2.12.2, https://www.handbook.fca.org.uk/handbook/EG/2/?view=chapter [hereinafter EG]. In such cases, the FCA may take disciplinary or other enforcement action if the firm fails to do so. *Id.*

[49] *Handbook on Rules and Guidance*, Fin. Conduct Auth., Supervision 15.3.8(3), https://www.handbook.fca.org.uk/handbook/SUP/15/3.html [hereinafter SUP].

[50] *Id.* at 15.3.17.

[51] *Id.* at 15.3.32.

[52] EG at 2.12.1.

company assisted the FCA in any factual investigation; and whether the company has taken remedial action.[53]

— **Voluntary Interviews:** The FCA may draw an adverse inference from refusal to cooperate in a voluntary interview; however, the failure to participate in such an interview is not necessarily itself a basis for disciplinary proceedings.[54]

European Union

In the European Union ("EU"), authorities at the national level likewise take cooperation into account in calculating fines in the context of civil and criminal investigations, and the European Commission ("EC") operates a leniency program that spans across the EU, by which it offers immunity or reductions in fines to companies that cooperate with investigations related to antitrust.

National Authorities

Authorities at the national level differ in the guidance provided for cooperating with civil and criminal investigations, as well as the credit awarded. Some illustrative examples include:

France. In France, cooperation by companies is particularly encouraged in the context of white collar crime investigations. Before 2017, there was little incentive for companies to come forward and cooperate with the French criminal authorities, because there was no effective legal mechanism to settle. This is one of the reasons why the French anticorruption legal framework (to take this example) had long been viewed as being deficient, ineffective and generally below international standards, particularly when compared to the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act (UKBA). That changed significantly as a result of the enactment at the end of 2016 of a sweeping anti-corruption reform ("*Loi Sapin II*") and recent efforts by French authorities to prosecute acts of corruption perpetrated abroad.

[53] *Id.*

[54] *Id.* at 4.7.3.

CASE STUDY:
FAILURE TO COOPERATE WITH THE FCA

In 2015, a global banking and financial services company was fined approximately $2.12 billion by U.S. regulators and £227 million by the FCA for misconduct related to Interbank Offering Rates ("IBOR") submissions and related systems and controls failures.[55]

In imposing this significant fine, the FCA explained that it was intended to show "how seriously we view a failure to cooperate with our investigations[.]"[56] Noting that the company had failed to deal with it "in an open and cooperative way,"[57] the FCA identified the following specific deficiencies:

— An "unacceptably slow and ineffective response to some of the [FCA]'s enquiries," which "prolonged the process of formal investigation significantly."[58]

— Misleading the FCA on "issues of importance."[59]

— Incorrectly telling the FCA that the Federal Financial Supervisory Authority in Germany (*Bundesanstalt für Finanzdienstleistungsaufsicht, "BaFin"*) had prohibited disclosure of a relevant report commissioned by the company, when BaFin had not.[60]

— Providing an inaccurate "formal attestation to the [FCA] stating that its systems and controls in relation to [certain IBOR] submissions were adequate at a time when no such systems and controls were in place."[61]

— Failing to provide "accurate, complete, and timely information, explanations and documentation to the [FCA]."[62]

A legal entity can now settle allegations of criminal misconduct with the special prosecutors tasked with fighting white collar crime (*the Parquet National Financier*, or "PNF"), by negotiating a *convention judiciaire d'intérêt public* ("CJIP"), which is akin to the U.S. deferred prosecution agreement. The purpose of this mechanism

[55] Press Release, Fin. Conduct Auth., *Deutsche Bank fined £227 million by Financial Conduct Authority for LIBOR and EURIBOR failings and for misleading the regulator* (Apr. 23, 2015), https://www.fca.org.uk/news/press-releases/deutsche-bank-fined-%C2%A3227-million-financial-conduct-authority-libor-and-euribor.

[56] *Id*.

[57] *Id*.

[58] *See* Fin. Conduct Auth., *Final Notice to Deutsche Bank AG* ¶ 2.3 (Apr. 23, 2015), https://www.fca.org.uk/publication/final-notices/deutsche-bank-ag-2015.pdf.

[59] *Id*.

[60] *Id*. ¶ 2.14.

[61] *Id*. ¶ 2.15.

[62] *Id*. ¶ 2.16.

is to (i) incentivize companies to come forward, with respect to offenses that are difficult to detect, while (ii) allowing companies to continue to qualify for public tenders and other forms of licenses in jurisdictions where applicable laws provide for automatic disqualification in the event of a criminal conviction. The first CJIP was concluded with HSBC Private Bank Suisse SA in October 2017, in relation to laundering of the proceeds of tax fraud ("*blanchiment de fraude fiscale*"), followed by the conclusion of two additional CJIPs related to acts of corruption in February 2018. More recently, Société Générale settled charges of corruption in connection with bribe payments to Libyan officials with both the U.S. and French criminal authorities.[63] This was the first coordinated resolution by U.S. and French authorities of a foreign bribery case.

Separately, cooperation may also be taken into account by the *Autorité des Marchés Financiers* ("AMF"), the regulator in charge of financial markets in France, when issuing sanctions against professionals under AMF supervision for breach of their professional obligations or against any individual or company for market abuse.

Germany. In Germany, BaFin, the supervisory and enforcement authority for the banking and insurance sectors and the financial markets generally, has issued sentencing guidelines (last updated in February 2017) for fines under the Securities Trading Act, for example for insider dealing and market manipulation charges and breaches of transparency requirements. Depending on the facts and circumstances of a particular case, BaFin can levy large fines on companies, amounting to up to 5% of group turnover.[64] Under the guidelines, cooperative conduct is a significant factor influencing the amount of the fine, and includes proactive self-reporting, assisting the authority in investigating and uncovering relevant facts, and remedial measures to avoid similar conduct in the future.[65] Other enforcement authorities in Germany also typically take cooperative conduct into account when levying fines on companies.

---

[63] In addition to the CJIP between the PNF and Société Générale S.A., the company entered into a deferred prosecution agreement with the DOJ. *See* Joon H. Kim and Elizabeth (Lisa) Vicens, et. al., *Société Générale Enters Into First Coordinated Resolution of Foreign Bribery* Case by U.S. and French Authorities (June 6, 2018), https://www.clearygottlieb.com/-/media/files/alert-memos-2018/societe-generale-enters-into-first-coordinated-resolution-of-foreign-bribery-case.pdf.

[64] *See* BaFin Fed. Fin. Supervisory Auth., Sec. Trading Act (Sep. 09, 1998) Federal Law Gazette I at Part 12 (Ger.), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/WpHG_en.html.

[65] *See* BaFin Ger. Fed. Fin. Supervisory Auth., *Guidelines on the Imposition of Administrative Fines for Offences relating to the German Securities Trading Act* 10-11 (Feb. 2017), https://www.bafin.de/SharedDocs/Downloads/EN/Leitfaden/WA/dl_lf_bussgeldleitlinien_2017_en.html;jsessionid=7A9172EF967971AEC37C4CBB62C1F3FC.1_cid381?nn=9646522.

Italy. In Italy, authorities provide limited guidance on factors considered in awarding credit for cooperation. In the civil context, authorities responsible for regulating the banking and financial market—such as the Bank of Italy and CONSOB (*Commissione Nazionale per la Società e la Borsa*)—have broad authority to enforce compliance with securities laws and regulations through investigations and imposition of administrative sanctions. In determining the sanctions to be issued, administrative authorities consider both the level of cooperation provided by entities and the remedial measures adopted to prevent further violations,[66] but do not otherwise specify cooperative efforts that should be taken, nor do they quantify cooperation credits. Nonetheless, in most cases where credit is awarded, cooperative conduct includes proactive self-disclosure of documents and information material to the underlying misconduct, and timely response to the requests of the authorities.

At the criminal level, prosecutors in Italy do not offer NPAs or DPAs, and criminal investigations conclude through judicial determination or through judicially-approved settlement. Judges do, however, consider a company's cooperative efforts in reaching a determination regarding the sanction to be imposed, and a company may receive credit if a judge finds that its cooperation mitigated the consequences of the misconduct or prevented further violations.[67] Similarly, in the case of individuals, a judge may award credit for cooperation by reducing a sanction up to one third under the Italian Code of Criminal Law.[68] In either case, it is in the sole discretion of the criminal judge to determine whether cooperation entitles the accused company or individual to a reduction of the sanction to be issued.

European Commission. Although most conduct is regulated at the national level within the EU, the EC regulates application of the EU antitrust rules, which can be found in the Treaty on the Functioning of the European Union, directives, and regulations. The EC's Directorate-General for Competition operates a leniency program offering immunity or fine reduction to companies that cooperate with authorities to detect cartel conduct affecting the European market. Under this program, total immunity is granted to the first cartel participant to "blow the

[66] *See* Decreto legislativo n. 58/1998 (TUF) (It.), art. 195 Sanction procedures. http://www.ecgi.org/codes/documents/testo_unico_eng.pdf.

[67] *See* Decreto legislativo n. 231/2001 (It.), art. 11 Determination of penalty policy § 1.

[68] *See i.d.* art. 62 Application of the sanction on request.

whistle,"[69] while other participants providing evidence that "represents 'significant added value' with respect to [that] already in the Commission's possession" may be eligible for a reduction of any fine that would otherwise have been imposed.[70] Notably, however, the immunity does not exclude the whistleblower's civil liability with respect to the victims of the cartel.[71]

Analogous leniency programs are also provided by EU Member States' national competition authorities. Notably, to achieve leniency at the national level in addition to the EU level, companies must apply for leniency to all competition authorities that could file a case against them.

When Should A Company Cooperate?

Companies should consider whether to cooperate as soon as a potential issue arises. The approach to determining a cooperation strategy depends on a number of factors, including the company's objectives, the perceived risks, the potential exposure of it and its executives, and the estimated likelihood of being awarded substantial cooperation credit. The decision to cooperate may also turn on the type of misconduct at issue and the company's role in the misconduct. For example, a potential target of an investigation may choose to take a different approach from a party that is merely a potential witness, where the costs of cooperation (but also its benefits) are likely to be significantly lower.[72] Because the company's early positions will likely set the tone with the relevant authorities for the entirety of the investigation, it is especially important to weigh the benefits and drawbacks of cooperation early on, choose a cooperation strategy, and remain consistent with that strategy as the investigation progresses. General considerations that may affect the decision of whether to cooperate at the outset of an investigation include:

---

[69] *See* Official Journal of the European Union, *Commission Notice on Immunity from fines and reduction of fines in cartel cases* (2006/C 298/11) Section II.A.8, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006XC1208(04)&from=EN. *See also id.* Sections II.A.9–13 (setting out the specific conditions for immunity).

[70] *See id.* at Section III.A.24. *See also id.* at Sections III.A.24–26 (setting out the specific conditions for reduction of fines).

[71] *See id.* at Section V.39.

[72] As set forth in the U.S. Attorney's Office Manual, a "target" is defined as a person "as to whom the prosecutor . . . has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant." Dep't of Just., *U.S. Attorneys' Manual* § 9-11.151 (Nov. 1997) ("USAM") (defining "target" for purposes of grand jury investigations). By contrast, a "subject" of an investigation is "a person whose conduct is within the scope" of the investigation, but who is not necessarily a putative defendant. *See id.* A "witness" is someone who can attest to facts or events. *See generally id.* § 9-11.154.

— ***Whether the relevant authorities already know of, or are likely to learn about, the conduct at issue.*** Regulatory or law enforcement authorities may independently discover conduct (or be likely to discover conduct) from a variety of sources, including whistleblowers, their own investigations into peer institutions, public media or press reports, or public statements a company makes in its mandatory disclosures. If it is a foregone conclusion that problematic conduct will be discovered (but has not yet been discovered), there is likely more to be gained by cooperating with a regulatory or law enforcement authority through self-disclosure or voluntary production of documents.

— ***The ability to gain substantial credit early on.*** A corollary to the above consideration is that authorities often will assign the most cooperation credit to companies that affirmatively notify them of events that they may not have learned of on their own.

— ***Whether the company is regulated by, or otherwise subject to the jurisdiction of the requesting authority.*** Although a company is likely to garner credit for assisting an investigating authority with obtaining information that it is otherwise unable to access, the company may want to consider whether that information would be beyond a regulatory or law enforcement authority's jurisdictional reach entirely, such that legal action would otherwise be precluded.

— ***Whether there was likely a breach of law.*** Where there was likely a clear breach of law, a company may seek to proactively cooperate as a preemptive attempt to mitigate liability that is otherwise a near certainty.

— ***Whether the company may be in a position to help advance the government's investigation of others, including individuals.*** Authorities are often focused on whether they can build cases against individuals as well as firms. Companies

considering whether to cooperate should thus be cognizant that they will likely be expected to provide factual information concerning the conduct of individuals.[73]

Another reason that a decision to cooperate should be made early in an investigation is that it will likely influence the company's position with respect to various investigative procedures, including:

— ***Document Collection.*** If a company plans to cooperate—and, thus, voluntarily produce documents to the investigating authority—it will need to give early consideration to what, if any, data protection laws may impact its ability to review and provide certain information.[74]

— ***Witness Interviews.*** Companies should consider whether they plan to make their employees available to be interviewed and what, if any, employee rights provisions in various jurisdictions may affect that decision.[75]

— ***Legal Privileges.*** Companies should also consider whether cooperation could implicate privileged or other confidential materials—for example, through a voluntary waiver or because a particular privilege is not recognized in a certain jurisdiction—and how, if at all, that likelihood affects how information is handled.[76]

[73] In September 2015, the DOJ issued a memo to address challenges it faced in prosecuting individuals involved in or responsible for corporate misconduct. See Deputy Att'y Gen. Sally Yates, *Individual Accountability for Corporate Wrongdoing* 2 (Sept. 9, 2015), ttps://www.justice.gov/archives/dag/file/769036/download. This memo, commonly known as "the Yates Memo" for its author, former Deputy Attorney General Sally Yates, applied to any investigation of corporate misconduct, and required full disclosure of an individuals' involvement in misconduct to qualify for *any* cooperation credit. *See id*. While the Yates Memo has been under review by the Trump Administration, Deputy Attorney General Rod Rosenstein recently endorsed its central premise, stating publicly that "any changes [to the Yates Memo] will reflect our resolve to hold individuals accountable for corporate wrongdoing." Deputy Att'y Gen. Rod J. Rosenstein, Dep't of Just., Keynote Address on Corporate Enforcement Policy, NYU Program on Corporate Compliance (Oct. 6, 2017), https://wp.nyu.edu/compliance_enforcement/2017/10/06/nyu-program-on-corporate-compliance-enforcement-keynote-address-october-6-2017/.

[74] *See* Chapter V: Data Privacy & Blocking Statues.

[75] *See* Chapter VI: Employee Rights and Privileges.

[76] *See* Chapter IV: Preserving Legal Privilege.

CASE STUDY: A FAILURE TO COOPERATE EARLY IN A DOJ INVESTIGATION

Refusal to cooperate in an investigation has been cited in assigning large fines to a company. For example, Alstom, a French power and transportation company, was fined $772 million to resolve criminal charges related to secret bribes. At the time, this was the largest criminal fine ever imposed in an FCPA enforcement action. According to the DOJ, the size of the fine was justified by Alstom's failure to voluntarily disclose broad misconduct, "refusal to fully cooperate with the department's investigation for several years," and "lack of an effective compliance and ethics program[.]" Indeed, although Alstom did eventually begin to cooperate thoroughly after the DOJ charged several of its executives, this was deemed insufficient to remedy its prior non-cooperation.[77]

CASE STUDY: WHEN COOPERATION WORKS

In June of 2016, the DOJ declined to prosecute Nortek, Inc. for possible violations of the FCPA, despite bribery by employees of Nortek's Chinese subsidiary. Reasons that were given for declination included:[78]

— Thorough internal investigation after its internal audit function identified the misconduct.

— Prompt voluntary self-disclosure.

— Identification of all individuals involved in or responsible for the misconduct, and provision of all facts relating to the misconduct to the DOJ.

— Agreement to continue to cooperate in ongoing investigations of individuals.

— Improvements to the company's compliance program and internal accounting controls.

— Full remediation of the misconduct, including terminating the employment of all individuals involved (including high-level executives).

— Disgorgement of unlawfully gained funds to the SEC.

[77] Press Release, Dep't of Just., *Alstom Sentenced to Pay $772 Million Criminal Fine to Resolve Foreign Bribery Charges* (Nov. 13, 2015), https://www.justice.gov/opa/pr/alstom-sentenced-pay-772-million-criminal-fine-resolve-foreign-bribery-charges.

[78] Letter from Daniel Kahn, Deputy Chief, Dep't of Justice, to Luke Cadigan, Esq., K&L Gates (June 3, 2016), https://www.justice.gov/criminal-fraud/file/865406/download.

Considerations For Determining Cooperation Risks

While there are many potential benefits to cooperation, it is not without risk. Accordingly, companies should be cognizant of the effects, costs, and risks associated with cooperation.[79] Relevant considerations may include:

— ***Expense.*** The expenses associated with cooperation, in legal fees and diverted personnel, may outweigh the potential benefits to be realized through cooperation credit. Further, companies may be faced with follow-on litigation brought by private parties after an investigation or a settlement is publicly disclosed, which are likely to present additional costs that may be substantial.

— ***Revelation of Misconduct.*** Information that is turned over through cooperation may alert the relevant authority to misconduct which it would not otherwise have investigated. Once the company begins to cooperate, it cannot control where the investigation will lead. For instance, information that is turned over to a regulatory agency may be provided to law enforcement divisions of that agency for prosecution. Cooperation may also result in an investigation's focus expanding into conduct the company did not envision at the start.

— ***Uncertain Outcomes.*** There is often no guarantee that cooperation will have the desired result. Indeed, an investigating authority could view the underlying conduct as more severe than the company would have expected, and may seek charges and fines beyond what the company anticipated or believes is appropriate.

In addition to the above considerations, it is important to remember that cooperation is but one factor in determining outcomes, and the amount, type, and degree of cooperation credit is often left to the discretion of the investigating authority. Government authorities may decline to award significant cooperation credit if they find that the company has been insufficiently cooperative, despite the company's best efforts. Moreover, the government may be hesitant to issue significant cooperation credit if the misconduct is particularly egregious or if the case is politically sensitive or newsworthy, even if the company provides extensive cooperation. Thus,

[79] Collateral considerations with respect to investigations are discussed in further detail in Chapter IX: Collateral Considerations.

in choosing to cooperate, a company may expend significant resources, time, and effort for an uncertain payoff.

Benefits of Cooperation

Cooperation can benefit a corporation, as well as its employees and shareholders, because it enables the authority to focus resources in a manner that may minimize disruption of the company's legitimate business operations, and, possibly, bring the investigation to a speedy conclusion.[80] Other benefits include:

— ***Reduced Penalties with the Investigating Authority.*** Cooperation credit may take the form of a deferred or non-prosecution agreement, a reduction in fines, or a reduction in jail sentence for a culpable individual. The degree and nature of cooperation credit will vary based on the facts and the investigating authority's approach to cooperation. For example, maximum cooperation credit is often reserved for companies that inform authorities about conduct of which they would not otherwise be aware. However, even short of such self-disclosure, U.S. authorities will often give some form of cooperation credit for other efforts to ease the burdens of investigation and encourage cooperation in the future.

— ***Reduced Penalties with Other Authorities.*** Steps that a company takes to cooperate with one regulatory or law enforcement authority may be communicated to another authority, and may be cited as a reason to offer cooperation credit by that other authority.[81] A company may also be credited for money paid to overseas regulators as part of a foreign investigation into the same misconduct.

[80] USAM § 9-28.700(B).

[81] The DOJ recently memorialized an anti "piling on" policy designed to limit the imposition of penalties by multiple regulatory agencies for the same misconduct in certain circumstances. *See* USAM § 1-12.100. Pursuant to this policy, "the adequacy and timeliness of a company's disclosures" and the company's cooperation with the DOJ are among the factors bearing on whether the imposition of multiple penalties is merited. *Id.*

CASE STUDY:
REDUCED PENALTIES DUE TO COOPERATION WITH ANOTHER AUTHORITY

In 2006, STATOIL, a Norwegian oil company, settled with both the SEC and the DOJ for FCPA-related violations. The DPA entered into by the DOJ and STATOIL specifically noted that the company had "fully cooperated with the [SEC]'s investigation" since it was contacted by the SEC.[82] Further, the DPA included a provision noting that the "DOJ will bring the cooperation of STATOIL and its compliance with its other obligations under this Agreement to the attention of [other] agencies and authorities if requested to do so by STATOIL and its attorneys."[83]

In the case of STATOIL, the company was assessed a $10.5 million penalty by the DOJ, but was credited $3 million for amounts paid to Norwegian authorities for the same bribery, bringing the overall DOJ penalty down to $7.5 million.[84]

— ***Maintaining Status as a Witness.*** Cooperation may protect a company's status as a witness, and prevent it from becoming a target of an investigation. However, the company may be required to assist authorities in building cases against individuals, who may be subjects or targets, to qualify for cooperation credit.

— ***Less Intrusive Investigation.*** There are a number of factors that may lead an investigating authority to be less-intrusive in its investigation of a cooperating entity. For instance, cooperating with an investigation may allow a company to help frame the issues by bringing useful evidence to the investigating authority's attention. This, in turn, may shorten an investigation. In addition, once counsel has built a rapport with the law enforcement or regulator's staff, the investigating authority may be more amenable to taking evidence by less intrusive methods, such as by attorney proffer or informal interviews, as opposed to written responses or on-the-record testimony from company employees. Finally, ongoing cooperation offers a window for continued advocacy with the attorneys conducting the investigation, including potentially, during settlement negotiations.

[82] Deferred Prosecution Agreement App'x A at 5, *United States v. Statoil, ASA*, No. 06-CR-960 (S.D.N.Y Oct. 13, 2006) (https://www.justice.gov/criminal-fraud/case/united-states-v-statoil-asa-court-docket-number-06-cr-960).

[83] *Id.* ¶ 26.

[84] *Id.* ¶ 19.

Prevention

When it comes to cooperation, an ounce of prevention may be worth a pound of cure. In addition to responding quickly when misconduct is discovered, companies with robust compliance and prevention programs in place will often be better positioned to receive cooperation credit once an issue arises. This is because such programs are often the best way to quickly detect and remediate issues, and can demonstrate to regulatory and law enforcement authorities that a company takes violations of the law seriously and has put forth its best efforts to prevent them from arising.

To maximize the likelihood of receiving cooperation credit, preventative measures should be robust and follow best practices as articulated by the relevant authorities.[85] An effective compliance program will allow a company to identify wrongdoing early on, so that the company can make a prompt disclosure to the government. This program should contain a clear process for escalating potential wrongdoing to a designated officer or team responsible for investigating the misconduct and deciding if any authorities need to be notified. Employees should be told that they must inform their supervisor or the designated agent if they observe any misconduct, or if they suspect illegal activity. If self-disclosure is appropriate, it should be made as promptly as possible.

[85] For example, the DOJ recently published a list of questions it may ask when examining the effectiveness of a corporate compliance program. *See* Criminal Div. Fraud Section, Dep't of Just., *Evaluation of Corporate Compliance Programs* (2017), https://www.justice.gov/criminal-fraud/page/file/937501/downloadhttps://www.justice.gov/criminal-fraud/page/file/937501/download.

PRACTICE TIP:
QUESTIONS TO CONSIDER IN REVIEWING COMPLIANCE PROGRAMS

- How effective are the procedures in place to detect, investigate, and remediate misconduct?
- How integrated into the program are senior and middle management?
- Are compliance personnel sufficiently resourced and independent?
- How robust is the process for implementing, communicating, executing, and improving compliance policies and procedures?
- How effective is the process for assessing risk, and using risk assessment information to inform the compliance program?
- Is the program well understood by employees and is adequate training and guidance provided to employees?
- What are the incentives for compliance and likely discipline for wrongdoing?
- Is there a periodic review and improvement to the compliance program?
- Does the company have a well-known and easily used whistleblower hotline?
- Does the program include established reporting chains in the event that wrongdoing is identified (both internally and to the government)?
- How does the company document corrective action taken under the program?

Maintaining a Record of Cooperation

It is important to maintain a clear record of all cooperative efforts and assistance provided during the course of an investigation, including the dates and content of any productions, presentations, or witness interviews or testimony. This record will help string together the various cooperation efforts into a streamlined narrative, which will likely serve as a crucial advocacy piece during the later stages of an investigation, where the decisions regarding penalties, leniency, and whether to decline prosecution altogether are imminent. The ability to reference the specific details of a company's cooperation, particularly those made at the outset of the investigation, may go a long way in reminding the relevant authorities of the company's good faith, and toward receiving credit where it is due.

Chapter VIII:
Public Relations & Message Management

Summary

First Public Relations Steps During a Crisis:

— Gather appointed stakeholders to coordinate messaging and ensure consistency across audiences.

— Identify groups who need to receive messaging, including employees, the public, regulators, customers, and creditors.

— Coordinate all disclosures with assistance and advice from counsel.

— Consider hiring a public relations firm quickly *in conjunction with* legal representation.

Key Points:

— Consider legal—and practical—factors of any public response.

— Decide whether to disclose—do you have a duty, and if not, is it the right move strategically in order to frame the message?

— Craft the disclosure—work to maximize its effectiveness while avoiding language that may lead to follow-on regulatory or litigation exposure.

— Work closely with counsel and public relations firms, and avoid waiving privilege by following important protocols.

Introduction

Frequently, the issues companies face during large-scale, oftentimes very public, crises require more than exclusively legal skills; they also require communications skills. The court of public opinion can have just as big of an impact—if not bigger—on a company's operations than any decision by a court of law. For example, when allegations of Wells Fargo's practice of opening fraudulent accounts came to light, it quickly lost 10% of its market capitalization for a $25 billion dollar loss[1]—but has faced roughly $800 million in fines and settlement amounts thus far, even after resolving major regulatory and civil cases.[2] The reputational impacts of these crises may be felt for years to come, especially if poorly handled. Indeed, failing to address a crisis promptly—and instead dealing with issues in an uncoordinated, piecemeal fashion—can lead to ongoing disclosures that not only complicate the legal response, but also keep the bad news in public view. By contrast, a well-designed litigation strategy frequently combines strictly legal arguments with public relations strategies.

This chapter discusses the process for how to handle the public relations aspects of any crisis, including how to weigh the practical and legal risks and benefits of any public response, whether voluntary or mandated, such as required disclosures under U.S. securities laws. For situations where a response is warranted, this chapter also contains factors to consider when crafting and delivering the message to limit risk. Further, these factors touch upon other details to keep in mind when executing these strategies, such as how to maintain legal privilege[3] and flexibility for any follow-on lawsuits or investigations. While each crisis is different, these elements and considerations should provide useful tools to manage the public response in a variety of situations.

---

[1] Lucinda Shen, *Wells Fargo's Shares are Now a Buy*, Forbes, Sept. 19, 2016, http://fortune.com/2016/09/19/wells-fargo-baird-buy-scandal/.

[2] *Consumer Financial Protection Bureau Fines Wells Fargo $100 Million for Widespread Illegal Practice of Secretly Opening Unauthorized Accounts*, Consumer Fin. Protection Bureau (Sept. 8, 2016), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-fines-wells-fargo-100-million-widespread-illegal-practice-secretly-opening-unauthorized-accounts/; Wells Fargo, *Wells Fargo Announces Agreement in Principle to Settle Class Action Lawsuit Regarding Retail Sales Practices*, Mar. 28, 2017, https://www.wellsfargo.com/about/press/2017/class-action_0328/; Stacy Cowley, *Wells Fargo Agrees to Settle With Shareholders for $480 Million*, N.Y. Times, May 4, 2018, https://www.nytimes.com/2018/05/04/business/wells-fargo-shareholder-suit-phony-accounts.html.

[3] Considerations regarding legal privilege are discussed in further detail in Chapter IV: Preserving Legal Privilege.

Assembling the Team

The first step, even before a crisis arises, is to assemble a crisis-response or communications team that will be available in the event of a crisis. Assembling a team in advance expedites any company response—with respect to issuing a public statement or deciding not to issue one—and defines responsibilities among stakeholders early to avoid confusion in execution. Below, we walk through considerations when choosing who to include on the communications team, including internal and external stakeholders.

Internal Stakeholders

The first members of the team should come from different cross-sections of the company. This group will ensure that the company's messaging is consistent across the company and that every potential audience is considered (such as the regulators, the public, and other employees). There are some obvious candidates for this group: senior management of the company, the general counsel's office, compliance, and senior members from any marketing, public relations and investor relations groups. Next, specific considerations for each crisis may dictate membership of other response team members. If certain subsidiaries or subdivisions play a prominent role in the crisis, the response team should consider including senior members from those groups, to help ensure a consistent message. For many investigations, especially those that may implicate management or Board members, it makes sense to create a special committee of the Board of Directors as an independent entity that can oversee the investigation and manage the crisis.

External Assistance

Once a crisis hits, the next decision will be whether to retain outside legal counsel and public-relations consultants to help handle the public response. For example, simple matters, such as possible violations caused by rogue, low-level employees and caught early by internal compliance may not ever require a large public response. Ultimately, like the decision to retain outside counsel generally in an investigation, the decision will turn on factors such as the complexity of the issues and nature of the exposure, including additional potential consequences. Of course, if a situation

calls for outside assistance, the quicker they are involved, the sooner they can help with messaging.

Deciding Whether and When to Make Public Statements After a Crisis

Having assembled and convened the crisis response team, one of the first steps during a crisis will be to determine what to say and when to say it. Like many aspects of responding to a crisis, the answer will depend on how it arises. For example, disclosing a public investigation in response to a Wells letter will likely be a careful, more deliberate disclosure than one arising after a high-profile public incident or indictment. Either way, in both instances companies need to evaluate both potential duties to disclose and risks of any public response. These considerations should encompass both legal and practical concerns, as, for example, business considerations to rebuild trust in a community or within a consumer base may trump legal considerations for follow-on law suits or investigations. Note that these considerations may also operate on different time-tables: a company may want to respond to unhappy consumers making a public outcry today, knowing that law suits may take years to resolve.

Practical Considerations to Playing Defense: Responding to Negative Press

When the investigation stems from an event garnering a lot of publicity, it may be worthwhile to make a statement to help shape the narrative and to express the appropriate concern and attentiveness to the matter. Thus, one strategy could be to begin resolving the issue as quickly as possible and make forceful assurances that the issue is being addressed, rather than letting bad news trickle out over a long period. However, the ability to execute this strategy will depend on what information is available to the company and the status of the investigation. Thus, in situations where companies are still in the early stages of determining what happened, a more generic statement acknowledging the situation but avoiding commenting on the facts may be more appropriate.

CASE STUDY:
VOLKSWAGEN DIESEL EMISSIONS

On September 18, 2015, the Environmental Protection Agency ("EPA") issued its first statements about Volkswagen's emission scandal resulting from "defeat devices" used to circumvent certain emission requirements. Volkswagen's early response tried to underplay the severity of the crisis, initially placing the blame on "mistakes of a few people" even though it quickly came to light that the misconduct went on for longer and involved more people than initially disclosed. By January, Volkswagen seemed willing to shoulder more of the blame. However, after National Public Radio did an initial interview with its CEO, who claimed the company never lied to regulators, he was forced to call back the next day to partially retract his statements.[4]

By failing to be upfront at the start of the initial investigations or making statements without complete information, the trickle of news from subsequent statements guaranteed that it stayed in the front pages. Further, in multiple instances these problems were compounded as the company had to walk back earlier statements about the scale of wrongdoing, making them seem simultaneously more culpable and less responsible. Thus, one option may have been for the company to have more fully disclosed the wrongdoing initially. Another option would have been to weather the storm of criticism caused by delaying any initial response, in favor of waiting for the results of its investigation.

Practical Considerations to Playing Offense: Managing the Message

Other crises will not arise in such a public way forcing a company's reaction, but will present the option for the company to make the initial disclosure in some manner, whether in a forceful public statement or in a limited disclosure as part of a larger set of statements. Either way, getting out in front of the issue offers the opportunity to control the story, and also to mitigate the impact of later bad news. Also, effective messaging may "creat[e] a climate in which prosecutors and regulators might feel freer to act in ways less antagonistic."[5]

[4] Pradnya Joshi & Danny Hakim, *VW's Public Relations Responses and Flubs*, N.Y. Times (Feb. 26, 2016), https://www.nytimes.com/interactive/2016/02/26/business/volkswagen-public-relations-flubs.html.

[5] *In re Grand Jury Subpoenas Dated March 24, 2003 Directed to (A) Grand Jury Witness Firm and (B) Grand Jury Witness*, 265 F. Supp. 2d 321, 326 (S.D.N.Y. 2003).

Of course, there may also be reasons to wait to disclose. For example, a public company facing the prospect of a regulatory investigation may wait to disclose the investigation, in order to avoid creating a future duty to disclose or update. It may also be premature to disclose if the investigation is at its early stages. The histories of regulatory investigations are rife with examples of investigations that otherwise might have died but that were given political and public fuel by premature disclosure. Additionally, when there is an opportunity to get ahead of the crisis and messaging, a premature statement may only worsen the situation if the underlying facts are unclear and the outcome uncertain. Especially early on in an investigation, it may be unclear how far up the management chain the conduct goes, thus certain confidence-inspiring messaging may be impossible or incorrect.[6] Finally, as discussed further below, if done incorrectly, any public statements may be misleading and could result in liability.[7]

Legal Duties to Disclose Investigations

Public companies operating in certain countries may face an additional factor to consider when choosing whether to disclose. This obligation may not be all-encompassing, however. For example, in the United States, public companies have no general duty to disclose information investors deem important.[8] There is also a presumption of confidentiality initially for formal investigations—hence the secrecy of criminal grand-jury investigations[9]—and Freedom of Information Act exemptions of law enforcement records, such as for the Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC" or "Commission").[10] Moreover, as long as public releases do not mislead, companies can take a reasonable amount of time to understand a problem and effectively address it.[11] Thus, companies can be

[6] For example, in the Wells Fargo case, the company's initial statements tried to cabin the wrongdoing to a few individuals, but later revelations that executives who were aware of the conduct left with substantial severance packages undermined its message regarding how serious the company was in addressing the issue. *See* James Rufus Koren, *Wells Fargo to pay $185 million settlement for 'outrageous' sales culture*, L.A. Times (Sept. 8, 2016), http://www.latimes.com/business/la-fi-wells-fargo-settlement-20160907-snap-story.html; Jen Wieczner, *How Wells Fargo's Carrie Tolstedt Went from Fortune Most Powerful Woman to Villain*, Fortune (Apr. 10, 2017), http://fortune.com/2017/04/10/wells-fargo-carrie-tolstedt-clawback-net-worth-fortune-mpw/.

[7] *See infra* Part IV(b).

[8] 17 C.F.R. § 240.10b-5(b) (2018); *see also Basic Inc. v. Levinson*, 485 U.S. 224, 239 n.17 (1988).

[9] Fed. R. Crim. P. 6(e)(2)(B).

[10] 5 U.S.C. § 552(b)(7) (2018).

[11] *Acito v. IMCERA Grp., Inc.*, 47 F.3d 47, 53-54 (2d Cir. 1995) (one-month delay before announcing third failed FDA inspection resulting in plant closure did not make a securities claim); *City of Rockton Ret. Sys. v. Avon Prods., Inc.*, No. 11 Civ. 4665(PGG), 2014 WL 4832321, at *24 (S.D.N.Y. Sept. 29, 2014) (three-month delay before announcing investigation following whistleblower letter was a "reasonable amount of time to evaluate potentially negative information").

strategic and need not disclose immediately every instance in which they undertake an investigation, whether by their own initiative or at the behest of a regulator. However, in certain situations, public companies have a duty to disclose material information about regulatory investigations.

For companies subject to its jurisdiction, the SEC has promulgated various reporting requirements for public companies to follow in their filings. Here is a brief summary of the most-pertinent Regulation S-K items that relate specifically to disclosing material information about regulatory investigations.

Regulation S-K Item 103

Item 103 states that a company must "[d]escribe briefly any material pending legal proceedings . . . known to be contemplated by governmental authorities."[12] However, this standard only requires the disclosure of *imminent* litigation. There is no duty to disclose litigation that is not "substantially certain to occur."[13] Thus, for example, receiving a subpoena or a Wells Notice about an SEC investigation does not necessarily trigger a disclosure requirement—that is, the fact of an investigation need not be disclosed.[14]

Regulation S-K Item 401(f)

Item 401(f) requires that in identifying and describing the background of its directors, registrants must describe certain events that are "material to an evaluation of the ability or integrity of any director, person nominated to become a director or executive officer of the registrant."[15] Included in the definition of such events is whether the person is "a named subject of a pending criminal proceeding."

---

[12] 17 C.F.R. § 229.103 (2018).

[13] *In re Lions Gate Entm't Corp. Sec. Litig.*, 165 F. Supp. 3d 1, 12, 18 (S.D.N.Y. 2016) ("[T]he securities laws do not impose an obligation on a company to predict the outcome of investigations.")

[14] *Id.*; *Richman v. Goldman Sachs Grp., Inc.*, 868 F. Supp. 2d 261, 273-74 (S.D.N.Y. 2012); *see also Westland Police and Fire Ret. Sys. v. MetLife, Inc.*, 928 F. Supp. 2d 705, 718 (S.D.N.Y. 2013) (holding that although pending state investigation was not a required disclosure under Item 103, it was a required disclosure under Item 303 because of potential business changes and fines resulting from state regulatory action).

[15] 17 C.F.R. § 229.401(f) (2018).

Regulation S-K Item 503(c) and Regulation S-K Item 303 (MD&A)[16]

Item 503(c) applies to prospectuses in securities offerings and is incorporated into periodic filings by Item 1A of the instructions to Forms 10-K and 10-Q. It requires a discussion of the most significant risk factors a company faces. Item 303 is a similarly broad regulation which also imposes a duty to "[d]escribe any known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations."[17] Thus in one instance, a court permitted claims to go forward for a failure to disclose ongoing criminal and civil investigations impacting a company's operations and financials.[18]

Duties to Correct and Update

Beyond formal regulations, case law in the United States has created additional requirements for public companies to correct or update prior communications in certain situations. A duty to correct previous communications may arise when the issuer of the statement discovers that the statement was inaccurate or misleading when made.[19] Similarly, even if a company's statements are accurate when made, a duty to update explicit or implicit forward-looking statements may arise if circumstances change and such statements become inaccurate or misleading. Certain circuits have recognized a duty to update but have construed it narrowly,[20] whereas the Seventh Circuit has held that there is no duty to update forward-looking statements.[21] This is an area in which the case law is in flux. Thus, companies should exercise extra caution when making statements early on in a crisis or investigation to avoid being forced into making a statement later when additional relevant facts are unearthed.

---

[16] 17 C.F.R. § 229.503(2018); 17 C.F.R. § 229.303 (2018).

[17] *Ind. Pub. Ret. Sys. v. SAIC, Inc.*, 818 F.3d 85, 94 (2d Cir. 2016) (citing 17 C.F.R. § 229.303(a)(3)(ii), *cert. granted sub nom. Leidos, Inc. v. Indiana Pub. Ret. Sys.*, 137 S. Ct. 1395 (2017), *cert. dismissed*, No. 16-581 (R46-032), 2018 WL 3026583 at *1 (U.S. June 18, 2018).

[18] *Id.*

[19] *Vacold LLC v. Cerami*, 545 F.3d 114, 121 (2d Cir. 2008); *Backman v. Polaroid Corp.*, 910 F.2d 10, 16-17 (1st Cir. 1990) (*en banc*).

[20] These are the First, Second and Third Circuits. *See Backman*, 910 F.2d at 16-17; *In re Int'l Bus. Machs. Corp. Sec. Litig.*, 163 F.3d 102, 110 (2d Cir. 1998); *Weiner v. Quaker Oats Co.*, 129 F.3d 310, 316-18 (3d Cir. 1997).

[21] *Gallagher v. Abbott Labs.*, 269 F.3d 806, 810-11 (7th Cir. 2001) (reasoning a duty to update would undermine purpose of periodic reporting regime).

CASE STUDY: BP OIL SPILL SECURITIES SUIT

Only days after the Deepwater Horizon oil spill, BP issued the first of multiple statements that the flow rate of the leak was about 5,000 barrels of oil per day. Eventually BP settled for $525 million with the SEC. The settlement noted that BP failed to update this initial flow rate disclosure despite internal data and third party data indicating that the actual indicated flow rate was ten to thirty times higher. If the company had not specified the flow rate in initial statements, it may not have been liable for failing to update the rate later.[22]

PRACTICE TIP: CHECKLIST OF U.S. SECURITIES LAW DUTIES TO DISCLOSE INVESTIGATIONS

- Item 103 – Investigations known to be pending or imminent.
- Items 503(c) and 303 – Risk factors and material impact on net sales.
- Item 401(f) – Events material to the integrity of directors.
- Duty to correct previous statements in light of new information that made it misleading at the time.
- Duty to update certain forward-looking statements.

For companies not subject to the jurisdiction of U.S. regulators—as well as for those which are—there may be other regulatory regimes that impose similar, or even quite different requirements. It is therefore essential at the start of a crisis to identify the different applicable rules and to plan a response cognizant of the potential duties by which the company is bound.

[22] Press Release, Sec. Exch. Comm'n., *BP to Pay $525 Million Penalty to Settle SEC Charges of Securities Fraud During Deepwater Horizon Oil Spill* (Nov. 15, 2012), https://www.sec.gov/news/press-release/2012-2012-231htm.

PRACTICE TIP:
CHECKLIST WHEN CRAFTING A STATEMENT

- Consider the audience. A message to corporate employees should differ from that delivered to a Congressional committee. Of course, while nuance may shape the delivery and content of each message for the corresponding audience, the messages must remain consistent.
- Whether to admit to wrongdoing is frequently a close question and requires careful examination and discussion. A well-crafted "admission" can earn regulatory credit and may staunch the bleeding in a public relations crisis. On the other hand, such admissions may be extremely harmful in litigation. A company may want to consider not admitting to or conceding anything that it would not concede in litigation. The short-term credibility gain may not be worth the long-term expense of having that statement constantly paraded about.
- Focus on policies—past and present. Explain how new policies will prevent similar occurrences in the future and how the company was always committed to avoiding such outcomes.
- Avoid unnecessarily pointing fingers. In some instances it may be necessary to explain what happened, but oftentimes trying to shift blame too overtly will backfire.[23] On the other hand, in an appropriate case, it might suitably frame the message.
- The reactionary "no comment" response may not always be the most effective. When consistent with other messaging on the topic, it may be better to avoid overly-legal language or the simple "no comment"-type of statements.
- Do not predict the outcome of an investigation.

Delivering the Message

After deciding to issue a statement, there are certain legal and practical considerations to keep in mind when drafting a statement's content. On the legal side, the primary goal will be to craft statements that are accurate and that limit exposure, and that protect privilege during investigations and suits. On the practical side, the message will need to be easily understood and crafted not to invite further scrutiny

[23] When Mylan came under scrutiny for its pricing of the EpiPen, its initial strategy of trying to deflect blame onto the healthcare system writ large served to fan the flames before antitrust charges. Charles Duhigg, *Outcry Over EpiPen Prices Hasn't Made them Lower*, N.Y. Times (June 4, 2017), https://www.nytimes.com/2017/06/04/business/angry-about-epipen-prices-executive-dont-care-much.html.

on the matter. Sometimes, these two goals may be in tension and the company will need to evaluate benefits and risks of achieving one goal at the expense of the other.

Practical Messaging Guidelines

Every crisis and brand is unique and thus companies should work closely with relevant public relations staff or consultants before drafting any public statement. There is no one-size fits all system for public messaging. However, below are some relevant considerations when putting together any statement.

Legal Requirements for Statements by Public Companies

Beyond drafting a statement to achieve the desired effect on the public, the statement should be tailored in consideration of legal requirements and ramifications. As an important example, if a public company subject to U.S. securities laws makes "misleading" statements—including, in certain instances, opinions with regards to its compliance with the laws—this can be the basis of independent legal action. Thus, even forward-looking statements expressing opinions regarding a crisis or investigation need to be carefully constructed to avoid being perceived as misleading. Therefore, statements should first be carefully evaluated by counsel before they are made public.

The authority for these requirements comes from SEC Rule 10b-5(b), which makes it unlawful for a company subject to the U.S. securities laws to make untrue statements, or statements which omit material facts.[24] Even opinion statements can be misleading (i) if the speaker does not actually believe them or (ii) if the speaker omits material facts about the inquiry into or knowledge concerning the opinion statement, even if the initial statement was not necessary.[25]

[24] 17 C.F.R. § 240.10b-5(b) (2018); *see also SEC v. Gabelli*, 653 F.3d 49, 57 (2d Cir. 2011) *rev'd on other grounds*, 568 U.S. 442 (2013) ("The law is well settled . . . that so-called 'half-truths' – literally true statements that create a materially misleading impression – will support claims for securities fraud.").

[25] *Omnicare Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, 135 S. Ct. 1318, 1326-27 (2015). After *Omnicare*, the Second Circuit has held that the standard does not require disclosure of facts counter to the opinion—merely that the defendant conducted a "meaningful" inquiry and in fact held that view. *Tongue v. Sanofi*, 816 F.3d 199, 214 (2d Cir. 2016).

CASE STUDY: BIOSCRIP

Be explicit in disclosures about investigations to avoid being misleading. After BioScrip received a subpoena, it released a statement in its 10-K SEC filing that there could be "no assurance that we will not receive subpoenas or be requested to produce documents in pending investigations or litigation from time to time." The court said that "those statements suggest [] [BioScrip] routinely responded to investigatory requests from the Government, but was not presently in the process of responding to such a request." However, at that time, it was under an investigation and had received such a subpoena. Thus, even if the statement was technically true, the court found it was likely to mislead prospective buyers.[26]

U.S. Private Securities Litigation Reform Act "safe harbor" for certain statements

The Private Securities Litigation Reform Act in the United States has a "safe harbor" that prevents certain forward-looking statements from being subject to U.S. securities suits.[27] These forward looking statements are insulated if: (i) the statements are accompanied by meaningful cautionary statements; or (ii) plaintiff fails to prove that the company had actual knowledge that the statement was false or misleading.[28] If the forward-looking statement is an oral statement, it should also reference a written cautionary disclosure. All cautionary disclosures should be specific as to the cautions and not use boilerplate language.

Thus, although a disclosure about an ongoing investigation (internal or otherwise) should not include a prediction about its outcome, language regarding the potential risks or next steps may fall under this umbrella. In one non-investigatory example, Chipotle's forward-looking statements regarding impact on earnings and risk of outbreaks during the initial period after an E. Coli breakout were protected by the safe harbor.[29] However, take care when drafting the statements—forward-looking provisions that are accompanied by overly vague or "catch-all" cautionary statements

[26] *In re BioScrip, Inc. Sec. Litig.*, 95 F. Supp. 3d 711, 727 (S.D.N.Y. 2015).

[27] 15 U.S.C. § 77z-2 (2018); 15 U.S.C. § 78u-5 (2018).

[28] 15 U.S.C. § 77z-2 (2018).

[29] *See Ong v. Chipotle Mexican Grill, Inc.*, No. 16 Civ. 141 (KPF), 2017 WL 933108, at *18 (S.D.N.Y. Mar. 8, 2017).

referring to risks generally are not "meaningful," and are therefore not protected by the safe harbor.[30]

PRACTICE TIP:
DO NOT CONTRADICT SETTLEMENT AGREEMENTS

It may be tempting, when settling on a no-admit or no-admit-or-deny basis, to issue a statement denying wrongdoing by implying that the company always maintained certain standards and practices. Be forewarned: regulators may force a withdrawal of such strongly-worded post-resolution statements, which then undermines the company's credibility. Thus, even a statement after a settlement on a no-admit-or-deny basis as benign as "we have maintained our standards, in market share as well as our reputation, in my view" have come under scrutiny.[31]

Privilege Considerations when Working with a Public Relations Firm

Hiring a dedicated crisis-management team and public relations firm can go a long way in mitigating the effects of damaging publicity. As discussed generally in Chapters I and IV, under the *Kovel* doctrine, communications with agents of attorneys are equally protected in many circumstances as communications with attorneys themselves.[32] This applies when attorneys (whether inside or outside counsel) hire a public relations firm specifically for the purposes of assisting in managing issues related to litigation.[33] Thus, whether it be by attorney-client privilege or the work-product doctrine, in order to protect privilege to the fullest extent possible, consider having outside counsel directly retain any public relations firm rather than the company doing so itself. Communications with a public relations firm hired to do general public relations work will not be as protected.

---

[30] *Asher v. Baxter Int'l Inc.*, 377 F.3d 727, 732 (7th Cir. 2004).

[31] Robert Khuzami, *Testimony on "Examining the Settlement Practices of U.S. Financial Regulators"*, Sec. Exch. Comm'n (May 17, 2012), https://www.sec.gov/news/testimony/2012-ts051712rkhtm#P77_13677. *See also* Floyd Norris, *Morgan Stanley Draws S.E.C.'s Ire*, N.Y. Times (May 2, 2003), https://www.nytimes.com/2003/05/02/business/morgan-stanley-draws-sec-s-ire.html.

[32] *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).

[33] *In re Grand Jury Subpoenas*, 265 F. Supp. 2d at 332; *Haugh v. Schroder Inv. Mgmt. N. Am. Inc.*, No. 02 Civ. 7955 (DLC), 2003 WL 21998674, at *4-5 (S.D.N.Y. Aug. 25, 2003) (documents drafted by counsel and sent to public relations consultant are not privileged but subject to work product protection).

CASE STUDY: PREMERA BLUE CROSS DATA BREACH

In October 2014, insurance provider Premera hired Mandiant, a forensic consulting firm to review its data management system. Mandiant discovered malware, and Premera promptly hired outside counsel in anticipation of litigation. Premera and Mandiant "entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel," but did not change the scope of work. After Mandiant issued a report, Premera announced the data breach to consumers. Then, during discovery of the subsequent class action litigation, plaintiffs sought, among other items, this report and other documents created by Mandiant about the breach. In opposing the motion to compel, Premera argued unsuccessfully these were protected under doctrines of work product and attorney-client privilege. Despite being supervised by outside counsel, the court held that because Mandiant was hired for business reasons and the scope of its work did not change, its work would not be protected under either doctrine, in comparison to other cases, like Experian and Target, where outside counsel separately retained an expert to conduct an investigation.[34]

[34] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1244-46 (D. Or. 2017).

Chapter IX:
Collateral Considerations

Summary

Key Points:

— When the first investigation starts, plan for the second: During the initial investigation, plan tactics and processes in anticipation of related subsequent regulatory inquiries and civil litigation for years to come. Consider all the downstream consequences of any concessions, both small (waiving privilege as to some documents) and big (admitting to wrongdoing in a settlement), to any regulator.

— Value consistency: When handling simultaneous investigations and regulatory requests, coordinate messaging to ensure efficiency and consistency in the messaging to the public, employees, civil litigants, and regulators.

— Respond to government and public attention: Sometimes a crisis or scandal invites legislative and government attention beyond the investigation due to public scrutiny. Be engaged and proactive with any subsequent legislative action or administrative rule-making to prevent over-correction.

First Steps After the Investigation Begins:

— Appoint a committee of team members to oversee and coordinate all related investigations and inquiries, even across jurisdictions.

— Assess exposure to civil and regulatory actions to prioritize and allocate resources effectively.

— Determine whether preemptive disclosure to other regulators or investors is warranted and at what stage.

Introduction

No one jurisdiction or government body has a monopoly on investigating and handling cross-jurisdictional crises. As a result, when a multi-jurisdictional crisis arises, companies often face related investigations by multiple regulators within and across jurisdictions. Settlements with one regulator can not only affect settlements with others, but may also entail nearly-automatic regulatory consequences, such as affecting a company's ability to continue to operate certain regulated business lines. Additionally, as the conduct that leads to these investigations comes to light, private plaintiffs will often bring follow-on civil litigation. Finally, depending on the publicity surrounding the event, the company may need to respond to legislative action or administrative rule-making.

This chapter describes how to plan ahead for these eventualities by identifying decisions with important downstream consequences that are not always apparent at the outset. Without careful planning, a company may risk accidental waiver of certain privileges, bind itself to certain statements made in an early settlement, or enter into agreements that can have serious consequences for its ability to conduct business. By keeping these consequences in mind, the cost and difficulty of defending multiple fronts and planning for the future can be better managed from the outset.

Planning for Multiple Investigations from the Outset

Be Organized During the Investigation and Productions

An investigation by a single regulator can take years to resolve.[1] The complexities and timelines only increase when multiple regulators across continents begin investigations at different times and progress at different paces. Civil litigation will also move at a different—and often slower—pace from the regulatory investigations.

However, once the regulatory settlements begin, private plaintiffs will receive a roadmap of the relevant facts and theories for their complaint, often expediting the fact-gathering process. Practically, this means the production of identical

[1] *See, e.g.*, Sec. Exch. Comm'n, *FY 2017 Congressional Budget Justification & FY 2017 Annual Performance Plan & FY 2015 Annual Performance Report* 37 (Feb. 6, 2017), https://www.sec.gov/about/reports/secfy17congbudgjust.pdf (stating that in FY 2015 the average time between opening an investigation and commencing an enforcement action was twenty-four months).

documents and disclosures about similar issues will be repeated with different parties over many years. Rather than reinventing the wheel in each instance, a company should generally aim to:

— Minimize the cost of investigating identical or similar questions.

— Ensure that regulators and litigants are given consistent answers to similar questions over the years.

PRACTICE TIP: HOW TO STAY ORGANIZED IN AN INVESTIGATION

— **Appoint and identify stakeholders** who will be responsible for following developments in all related civil and regulatory cases, even across jurisdictions. In a large multi-national institution, there will likely be different groups or divisions responsible for managing different types of litigation risk based on jurisdictional and subject-matter consideration. Thus, as a simple example, an office in London may oversee European litigation generally, whereas the New York office oversees the American litigation. Appointing a committee will help ensure that the members update one another on major developments and are aware of strategic concerns outside of their own jurisdictions regarding the matter.

— **Track which data was collected by whom.** Because of differing theories and burdens of proof, the multiple regulatory entities and civil litigants will likely have different questions about technical details that are difficult—both in the amount of time it takes and in the level of disruption—to reproduce years later if it was not collected initially. For example, a civil litigant may ask how certain financial data was collected and what it contains years after it was collected for a regulator. Similarly, certain hard-to-produce data may never have been collected at all. It will be impossible to anticipate everything that will be important to every party at every point in time. However, to be in the best position to answer these questions at minimal cost and disruption, track the origin of each data set and why certain decisions with regards to document collection and production were made.

— **When tracking the origin of collected documents, take note of the data privacy issues for each jurisdiction.** Just because the data was produced to one regulator in one country, that does not mean it can be produced without issue to a different regulator in a different country. At a minimum, in many instances a protective order or separate agreement may need to be negotiated regarding that

data.[2] In addition, exercise thought with respect to the movement of documents from one jurisdiction to another. The careless movement of documents from one jurisdiction to another (even to a law firm in the second jurisdiction) may result in the loss of data privacy protection that otherwise might shield these documents from production to a regulator.

- **Keep detailed privilege and production logs.** As discussed below, regulators or civil litigants in an investigation or litigation that lags behind the initial investigation will likely begin discovery by asking companies to produce every document previously produced to regulators. This is known as "cloned discovery." Different courts have different approaches with respect to such requests; some courts permit them while others do not. When permitted, these productions will often be accompanied by privilege logs, but specific grounds for withholding documents may differ jurisdiction-to-jurisdiction and may need to be updated for each matter. Further, as regulators make idiosyncratic requests relevant to their jurisdiction or theory that are not disclosed, the "cloned discovery" may not be entirely synced among parties. Thus, to avoid accidentally withholding or disclosing documents, make sure there is one detailed "master" production log accounting for the different regulator-specific documents and privilege decisions.
- **Update prior answers when subsequent investigations disclose additional information.** During investigations into similar conduct, it is important to coordinate responses and maintain a consistent message among all regulators, including updating prior answers and productions to regulators when that information is newly made available to other regulators. Even when one regulator has not specifically asked for an item, it may make sense to produce it to that regulator when a company is producing it to respond to another regulator if it is likely to be or become relevant to its inquiry. When generating a document for a regulator containing factual information, it is also frequently useful to note that it is based on the best available information at the time and to correct such documents based on new information.
- **Reassess cooperation and preemptive disclosure choices.** As discussed further below, as the investigation brings more information to light, periodically reevaluate whether preemptive disclosure to other regulators may be beneficial.

[2] Data privacy is discussed in further detail in Chapter V: Data Privacy & Blocking Statutes.

Consider Downstream Consequences of Production and Settlement

Even if facing seemingly separate investigations from regulators in different jurisdictions, a company should assume decisions made in one will still impact investigations in another. Two major areas where these downstream consequences are significant are during document productions and when settling with a regulator. Generally, a company should not expect to produce documents "only" to a certain regulator or to cut a less-than-favorable deal in order to resolve a particular (often "minor" investigation). Similarly, without careful consideration, decisions made in order to resolve a matter with one regulator will dictate the terms with other regulators down the line.

Handling Cloned Discovery and Privilege Considerations

Document productions to one regulator do not happen in a vacuum specific to that regulator. In fact, many regulatory discovery requests will be very broad to start, but at a minimum most will request "cloned discovery," requiring the company to produce all documents previously produced in the context of the investigation to other regulators. Civil litigants will take the same approach and attempt to seek discovery of all materials produced to regulators. Some courts grant these requests on the view that "[t]he burden on the defendants is slight when a defendant has already found, reviewed and organized the documents."[3] Others do not, based on the competing view that civil litigants should not be able to piggyback on the work of government regulators.[4] Regardless, companies should anticipate and plan for the possibility of cloned discovery from an early stage, and work with counsel to develop arguments for limiting cloned discovery when it is later requested by regulators or civil litigants (for example, based on data privacy, privilege, jurisdiction, or burden).

[3] *In re Bank of Am. Corp. Sec., Derivative, & Emp. Ret. Income Sec. Act (ERISA) Litig.*, No. 09 MDL 2058 (DC), 2009 WL 4796169, at *2 (S.D.N.Y. Nov. 16, 2009) (lifting the automatic stay of discovery of the PSLRA due to prior investigations) (internal quotation marks omitted).

[4] *See, e.g.,* Order Denying Volkswagen-Branded Franchise Dealers' Motion To Compel, *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Products Liab. Litig.*, No. 3:15-md-02672 (N.D. Cal. Apr. 24, 2018), ECF No. 4996.

PRACTICE TIP:
LIMITING CLONED DISCOVERY

Although some courts grant cloned discovery and such discovery may be useful in some circumstances, companies should still consider planning for and fighting off discovery requests seeking "all" productions to and communications with regulators during the investigation. In one instance, the court denied plaintiff's initial request as overbroad, and subsequently granted plaintiff's limited request for a "targeted subset of regulatory materials, including white papers, presentations, written memoranda, or briefs shown or provided."[5] Further, planning for potential requests for cloned discovery by relying on oral presentations to regulators, where possible, may be an effective means of limiting the impact of clone discovery requests.

Another consideration when producing documents is whether the company is waiving a privilege. Producing a document to one regulator may waive the privilege to that document—or worse, to an entire subject matter—in the future.[6] Whether it will result in a waiver depends, in part, on whether the company had a privilege in the first place and whether it asserted that privilege or voluntarily produced. Because waiving privilege may grant cooperation credit during settlement negotiations,[7] it may, in some cases, be a worthwhile strategy. Ultimately though, the decision to produce privilege communications should only be made after careful consideration of the pros and cons of disclosure relevant to *the entire set of investigations* rather than the considerations relevant only to a specific regulator. In particular, companies and their counsel should consider different privilege standards across jurisdictions, along with the importance of disclosing privileged communications to obtain cooperation credit with regulators, the ability to maintain flexibility for future investigations or litigation by *not* disclosing privileged communications, as well as whether there are alternative ways to satisfy a regulator without actually disclosing privileged communications. For example, counsel may be able to present regulators with non-privileged facts learned during the course of an investigation that can get regulators most, if not all, of what they need without waiving privilege.

---

[5] *Alaska Elec. Pension Fund v. Bank of Am. Corp.*, No. 14 Civ. 7126 (JMF), 2017 WL 280816, at *1 (S.D.N.Y. Jan. 20, 2017).

[6] *E.g., In re Grand Jury Proceedings*, 219 F.3d 175, 182–83 (2d Cir. 2000) ("[A] party cannot partially disclose privileged communications or affirmatively rely on privileged communications to support its claim or defense and then shield the underlying communications from scrutiny by the opposing party."). *See also* Chapter V: Data Privacy & Blocking Statutes, discussing privilege considerations in further detail.

[7] *E.g.*, USAM 9-28.700; Federal Sentencing Commission, Guidelines Manual § 8C2.5 ¶ 13 (2016), https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2016/GLMFull.pdf. Cooperation is discussed in further detail in Chapter VII: Cooperation.

PRACTICE TIP: UNIQUE COLLATERAL PRIVILEGE CONSIDERATIONS—HANDLING A CONGRESSIONAL INVESTIGATION

When facing a congressional investigation, there are unique difficulties in maintaining and preserving legal privilege for related regulatory investigations and subsequent private actions. Chiefly, congressional committees do not always respect the invocation of attorney-client privilege and work product doctrines, and there are limited options to challenge such determinations, given the lack of court review.[8] And documents produced in these investigations are often referenced or contained within congressional investigative reports following the investigations. Litigants then request or attempt to use these documents, on the theory that privilege has been waived through disclosure to Congress.[9]

However, producing documents to Congress may not automatically waive privilege. Courts have held that producing documents under a subpoena demand is often considered an involuntary disclosure that will not waive the privilege as to other litigants.[10] Yet, to avoid waiving the privilege, a company may need to show it at least attempted to assert privilege or resist producing them to Congress initially before complying.[11] This standard raises difficulties of litigants that may want to avoid a formal subpoena from Congress, and voluntarily produce documents.[12] In such circumstances, voluntary responses to Congress raises similar waiver and confidentiality considerations, and should be framed and negotiated in such a way as to limit the risks of waiver to the greatest extent possible.

[8] *See generally* Todd Garvey & Alissa M. Dolan, Cong. Research Serv., *Congress's Contempt Power and the Enforcement of Congressional Subpoenas: Law, History, Practice, and Procedure* 61 (2014), https://www.everycrsreport.com/files/20140410_RL34097_e1c05978a98ae4be23d3a3d973c553198c9dda72.pdf ("In the end, of course, it is the congressional committee alone that determines whether to accept a claim of attorney-client privilege.").

[9] *See, e.g., Spears v. First Am. eAppraiseIT*, 75 F. Supp. 3d 208, 212 (D.D.C. 2014).

[10] *Id*. at 212–13 ("[E]ven if the disclosure of documents were considered voluntary, because the documents were provided under seal by the OTS to the Senate PSI, this Court cannot reason that the disclosure was inconsistent with the maintenance of secrecy.").

[11] *Anaya v. CBS Broad., Inc.*, No. 06 Civ. 476 (JB) (KBM), 2007 WL 2219394, at *10 (D.N.M. Apr. 30, 2007) ("It is fair for a court to require the witness show that some serious effort was made to convince the Chair/and or the committee itself to recognize the privilege claims being asserted.") (citation omitted).

[12] *C.f., United States v. Philip Morris Inc.*, 212 F.R.D. 421, 426 (D.D.C. 2002) (producing documents day after receiving subpoena considered voluntary and a waiver).

Settlement Timing

Choosing when to begin settlement discussions with regulators may have cascading effects. For example, one of the factors considered by federal prosecutors when shaping settlement demands is the existence of related settlements for the same conduct.[13] Thus, where possible, a company should consider the sequence to maximize credit among regulators who may consider prior and related settlements.[14] However, settling with one regulator will likely invite scrutiny from other regulators or civil plaintiffs. Thus, also consider coordinating settlements to effect a global settlement among multiple regulators or with multiple defendants simultaneously if there is a joint-defense group. This may even be possible on a cross-jurisdictional basis.[15]

PRACTICE TIP:
MAXIMIZING COOPERATION CREDIT

Even when a global settlement may not be possible it is still important to coordinate active and potential investigations before settlements. In order to maximize cooperation credit where relevant, before the first settlements or investigations are made public, consider whether preemptively reaching out to regulators who might otherwise respond to an announcement and begin an investigation is the proper course of action. Especially when the investigation involves multiple defendants, consider reaching out to regulators who grant additional credit for being "first in line" even before news of the investigations begins to leak.

But be careful. It is a balancing act between engaging in preemptive disclosure to gain cooperation credit and engaging regulators who might not otherwise have taken action but for the disclosure.[16]

[13] *See* Dep't of Just., *U.S. Attorneys' Manual* § 9-28.300 (Nov. 1997) ("USAM"). In fact, the Department of Justice ("DOJ") recently announced an anti "piling on" policy designed to avoid penalizing companies repeatedly for the same conduct in certain circumstances. *See* Deputy Att'y Gen. Rod J. Rosenstein, Dep't of Just., Remarks at the American Conference Institute's 20th Anniversary New York Conference on the Foreign Corrupt Practices Act (May 9, 2018).

[14] *See*, for example, the Statoil settlement discussed in Chapter VII: Cooperation.

[15] *See, e.g.*, Press Release, Sec. Exch. Comm'n, *Petrochemical Manufacturer Braskem S.A. to Pay $957 Million to Settle FCPA Charges* (Dec. 21, 2016), https://www.sec.gov/news/pressrelease/2016-271.html (noting a nearly billion dollar global settlement with the "SEC, U.S. Department of Justice, and authorities in Brazil and Switzerland"); Press Release, Sec. Exch. Comm'n, *SEC Sanctions Statoil for Bribes to Iranian Government Official* (Oct. 13, 2006), https://www.sec.gov/news/press/2006/2006-174.htm (announcing a simultaneous settlement with the SEC and deferred prosecution agreement with the DOJ and U.S. Attorney's Office for the Southern District of New York).

[16] Considerations regarding cooperation are discussed in further detail in Chapter VII: Cooperation.

Negotiating Settlement Language—Limiting Prejudicial Language

When settling with a regulator, it is vital that any statement of facts accompanying the settlement, and especially any admission of wrongdoing, is as limited and narrow as possible. Even when settling on a "neither-admit-nor-deny" basis—which prevents future litigants from admitting evidence of that settlement as proof of liability[17]—limiting the tone and scope of the factual allegations is important. Future regulators and civil litigants will look at these prior documents as a starting point when considering their theories. Some courts will permit plaintiffs to rely even on unadmitted allegations in supporting a claim for relief.[18]

Most beneficially, settlements that admit no wrongdoing and contain no harmful facts can be used affirmatively in negotiations with other parties. Of course, getting a settlement without an admission may be easier said than done, depending on governmental or public pressure on obtaining admissions of wrongdoing.[19] However, make sure, to the extent that there is negative language regarding corporate conduct, to limit, where possible, the extent to which the company is restricted in what positions it can take in subsequent civil litigation.[20] One issue to keep in mind relates to the legal standards that civil litigants and regulators in other jurisdictions will need to satisfy to bring a claim. Frequently, it may be possible to use language that satisfies one regulator without admitting to allegations that constitute a violation in a second jurisdiction.

---

[17] *See, e.g., United States v. Cook*, 557 F.2d 1149, 1152, 1155 (5th Cir. 1977) (holding that the DOJ was not permitted to admit into evidence a prior neither-admit-nor-deny settlement with the SEC).

[18] *In re Fannie Mae 2008 Sec. Litig.*, 891 F. Supp. 2d 458, 471 (S.D.N.Y. 2012), *aff'd*, 525 F. App'x 16 (2d Cir. 2013) (permitting plaintiffs to rely on SEC's complaint and non-prosecution agreement in pleadings) (citing *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887 (2d Cir. 1976)).

[19] *See* Mary Jo White, Chairwoman, Sec. Exch. Comm'n, Address at the Council of Institutional Investors Conference: Deploying the Full Enforcement Arsenal (Sept. 26, 2013), https://www.sec.gov/News/Speech/Detail/Speech/1370539841202 (outlining new admissions policy when settling claims with the SEC); Letter from Sen. Elizabeth Warren to Sec. Exch. Comm'n Chair Mary Jo White 8 (June 2, 2015), www.warren.senate.gov/files/documents/2015-6-2_Warren_letter_to_SEC.pdf (claiming that SEC waivers allows banks "to continue to enjoy special privileges under the securities laws despite the deep breaches of trust and evident mismanagement displayed").

[20] Thus for example, regulatory policy in the Commodity Futures Trading Commision ("CFTC") typically results in a provision in any settlement order stating "nothing in this provision shall affect" the "right to take legal positions in other proceedings to which the Commission is not a party." *See, e.g.*, *In re Barclays PLC*, CFTC No. 12-25, 2012 WL 2500330, at *36 (June 27, 2012).

Negotiating Settlement Language—Developing Advantageous Language

Beyond limiting negative language, try to include as much positive language as possible in the settlement that can be used offensively by the company in related future proceedings.

PRACTICE TIP:
INCORPORATING BENEFICIAL LANGUAGE INTO A SETTLEMENT

Consider an example settlement regarding conduct of a rogue employee. Include language, as applicable, highlighting:

- The company's robust compliance programs.
- The company's cooperation and self-reporting.
- Lack of knowledge by senior management at the company.
- Losses to the company caused by the rogue employee.
- The company's efforts to make possible victims whole.

Although this language may not prevent future litigation, it will help set the narrative and frame the conduct at issue in a way that is most beneficial to the company.

Negotiating Fines and Settlements

Like the settlement language, a major part of any settlement is the monetary sanction, which may be seen as a signal to future litigants about what to expect. The first settlement amount may be seen as a "floor" that future regulators compete with during settlement negotiations. Depending on the regulator's jurisdiction, consider trying to classify as much of the monetary penalty as possible as restitutionary or disgorgement awards instead of fines or penalties. Courts may rely on general equitable principles to prevent double recoveries to the same parties for the same conduct. Thus, restitutionary or equitable awards may foreclose or limit certain

types of follow-on civil litigation that address the same conduct.[21] In addition, regardless how the financial sanction is characterized, if monies flow to victims, that might limit the company's financial exposure in parallel private litigation. Conversely, payments toward civil settlements may reduce certain types of awards from regulators or limit their suits entirely if they bring similar claims on behalf of consumers.[22] It is also useful to be mindful of the tax and insurance consequences of a financial sanction. While oftentimes a penalty might not be tax-deductible or insurable, that rule is not uniform and there are exceptions. Slight changes in language may make a big difference in a company's ability to take a tax deduction or recover from an insurer.[23]

[21] *See, e.g., Imber-Gluck v. Google Inc.*, No. 5:14 Civ. 01070 (RMW), 2015 WL 1522076, at *2 (N.D. Cal. Apr. 3, 2015) (citing *Kamm v. Cal. City Dev. Co.*, 509 F.2d 205 (9th Cir. 1975)) (denying class certification because the class was better served through the FTC settlement, which refunded customers for its wrongdoing); *Litton Indus., Inc. v. Lehman Bros. Kuhn Loeb Inc.*, 734 F.Supp. 1071, 1076-77 (S.D.N.Y. 1990) (civil settlement reduced by any profits already disgorged to SEC in prior action).

[22] *See, e.g., SEC v. Palmisano*, 135 F.3d 860, 863-64 (2d Cir. 1998) (disgorgement award offset by payments made in criminal case); *People ex rel. Spitzer v. Applied Card Sys., Inc. (In re People ex rel. Spitzer)*, 11 N.Y.3d 105, 124-25 (2008) (New York Attorney General was barred by res judicata from seeking additional restitution due to prior California class action). *But see SEC v. Shah*, No. 92 Civ. 1952 (RPP), 1993 WL 288285, at *4-5 (Jul. 28, 1993) (no offset to regulatory fine for civil settlement because recoveries were under different theories of improper gain).

[23] *See* Diana L. Wollman and Jonathan Gifford, *IRS Issues Guidance on Deductibility of Settlement Payments Under New Law*, Cleary Enforcement Watch (Apr. 6, 2018), https://www.clearyenforcementwatch.com/2018/04/irs-issues-guidance-deductibility-settlement-payments-new-law/; Diana L. Wollman *et al., Settlement Payments Under the New Tax Reform Law*, Cleary Enforcement Watch (Feb. 21, 2018), https://www.clearyenforcementwatch.com/2018/02/1962/.

PRACTICE TIP: NEGOTIATING FINES

1. **Find the right tone:** If the negotiation is with an industry regulator that the company will have continued relations with, it may make sense to develop a less adversarial tone during the negotiation to preserve the relationship. At the same time, it may be wise to be more aggressive when negotiating the first settlements, given their potential impacts on future resolutions.
2. **Using Prior Settlements:** If the company's prior settlements with other regulators for the same conduct have favorable language and are still applicable (i.e., no other relevant conduct has since come to light), use them affirmatively during negotiations. If the prior settlements are negative, avoid them or distinguish them based on the different regulator's powers or jurisdictional hooks. For example, an antitrust regulator and a banking regulator might both look into a conspiracy scheme, but from vastly different angles and with different goals in mind. The banking regulator may focus more on systems and controls and may not differentiate significantly between unilateral and multilateral conduct, whereas the competition regulator may focus more on meetings and language suggesting agreements among competitors.
3. **Using Related Settlements:** If this settlement is part of a multi-defendant investigation, differentiate the company from other parties using other publicly available settlements and fact-finding as a way to lessen the fine in comparison. Even in situations where there are no co-defendants, it may be useful to compare the situation at hand with recent prior settlements with that regulator, or for similar conduct, to ensure consistency.
4. **Using Prior Settlements Against Other Companies:** Settlements the regulator has entered in other matters can be an important benchmark. Study settlements early in an investigation and be mindful of the facts that the regulator has deemed important in developing the factual records, making arguments, and providing cooperation.

Anticipating, Avoiding, and Coordinating Collateral Consequences

In certain industries (and especially in the securities industry), admissions of wrongdoing in a settlement, the filing of an indictment, the entering of a judgement, or the entering of an order from a Self-Regulatory Organization might trigger collateral consequences that require the company to apply for waivers or exemptions in order to avoid disqualifications or continue conducting certain business activities.[24] Details that seem insignificant may lead to far-reaching regulatory consequences. However, minor adjustments to the language of the settlement can often avoid triggering these consequences. In a regulatory climate where the process of obtaining waivers has become more protracted and less certain,[25] it is important to try to avoid being subject to this process in the first instance. Therefore, a company should begin thinking about these potential consequences from the outset of an investigation and should consult experienced counsel early on to make sure these collateral regulatory consequences are considered and anticipated.

PRACTICE TIP:
CONSIDERING THE RELATIONSHIPS BETWEEN REGULATORS

Regulators may not be averse to incorporating changes in settlement documents that will avoid triggering collateral consequences imposed by other agencies. The settling regulator may not be concerned with those consequences, or may even want to avoid becoming subject to other regulators' timelines.[26] Since the regulator may be open to negotiating these points, companies should not be hesitant to introduce such revisions to the settlement language.

[24] As one important example, large financial institutions subject to an enforcement action must request an exemption with the SEC to continue to be considered a "well-known seasoned issuer," which grants them certain conveniences when registering securities for offer and sale. *See* 17 C.F.R. § 230.405 (2018); Mary Jo White, Chairwoman, Sec. Exch. Comm'n, Remarks at the Corporate Counsel Institute: Understanding Disqualifications, Exemptions and Waivers Under the Federal Securities Laws (Mar. 12, 2015), https://www.sec.gov/news/speech/031215-spch-cmjw.html (discussing exemptions and waivers under federal securities laws). As another example, FINRA will revoke the membership of any entity subject to enforcement actions under the "statutory disqualification" requirement in 15 U.S.C. § 78c(a)(39), although it has a process for entities to seek a waiver and maintain membership. *See, e.g., Mathis v. SEC*, 671 F.3d 210, 216 n.5 (2d Cir. 2012). In addition, government agencies may also refuse to contract with companies that have a conviction or civil judgment for certain misconduct. *See generally* 48 C.F.R. § 9.4 (2018).

[25] *See, e.g.*, Emily Flitter, *Settlements for 3 Wall Street Banks Hold a Silver Lining*, N.Y. Times, Feb. 1. 2018, https://www.nytimes.com/2018/02/01/business/banks-settlements-waiver-cftc-sec.html.

[26] *See id.* (quoting a Commodity Futures Trading Commission ("CFTC") spokeswoman as commenting that "forcing banks to wait for waivers had kept the C.F.T.C. from finalizing settlement agreements. 'The S.E.C.'s waiver process has taken up to nine months,' she said. 'In these cases, this has delayed C.F.T.C. enforcement actions, which otherwise would have been resolved, for almost a year.'").

To this end, at an early stage in negotiating a resolution with a regulator or litigant, ideally before seeing the first draft of the language of a settlement, it is important to conduct a review in consultation with counsel experienced in this area, using existing knowledge of the company's business as well as past company settlements in order to identify the potential consequences of entering into the settlement. After this review, the company can propose changes to the settlement language, or the addition of a statement of disqualification, that will avoid triggering these consequences, thus obviating the need to seek exemptions or request waivers.

If it is not possible to avoid triggering regulatory consequences when entering into a settlement, the company should work with counsel to review the relevant waivers and exemptions and resolve them before settling in order to avoid disrupting corporate units or triggering any separate legal reporting requirements. In particular, it is important to manage the timing of the finalization, approval and announcement of the settlement, if possible, to give the company time to engage in advocacy with the relevant regulators and negotiate any waivers and exemptions to be received before the settlement is entered. Raising the need for more time to seek waivers and exemptions in the "eleventh hour" can result in the settling regulator requesting additional sanctions or declining to delay the settlement, which in turn risks potential negative market and reputational impacts associated with the consequences being publicized.

Navigating Simultaneous Requests from Multiple Authorities

During a large, multi-jurisdictional investigation, there will be multiple regulators receiving productions at the same time. At any given time, some of these regulators may be more engaged than others. However, regardless of which regulators are driving the productions, make sure that, where appropriate, responses to multiple authorities are coordinated and considered strategically to ensure goodwill and maximize cooperation credit. Thus, for example, where possible, relevant productions should be made to all investigating regulators simultaneously and should be appropriately framed in dialogue or correspondence. This coordination may even help reduce costs for the company during each production. If the productions going to regulators become out of sync or if discussions with regulators about the productions vary in substance or context, it may reflect poorly on the cooperation of the company. Regulators may speak to one another regarding an investigation

and compare notes.[27] Thus, if one regulator views itself as consistently being treated differently, it may extend less goodwill in the future.

Conversely, just because regulators *may* talk does not mean that companies should assume that they *do*. For example, materials produced in the context of a criminal grand jury investigation cannot be shared with the civil department or civil regulatory agencies,[28] so companies should not assume productions made in part of a related proceeding will automatically be shared with all parties. Nor should a company assume that one regulator will be comfortable that its communications with the company will be shared with a second regulator. While it might be important to keep multiple regulators all on the same footing, it is equally important to be sensitive to the concerns of each regulator that the course and direction of its investigation be kept confidential.

Types of Follow-On Civil Litigation

Consider the possibility of follow-on civil litigation once the conduct is uncovered and an investigation begins. Depending on the underlying conduct, whether it has caused harm, and the identity of those affected, suits may arise from consumers, shareholders, or even competitors. Further, the monetary demands from these cases may far exceed the fines a company faces from regulators.[29] Indeed, in some cases, private litigants may even be able to obtain double or treble damages.

There are multiple types of follow-on litigation, depending on the nature of the underlying conduct. Consumers, shareholders (securities violations and shareholder derivatives suits), competitors (antitrust and competition suits), and others who may have been affected by the wrongdoing can rely on the investigative findings as a roadmap for their complaint. As noted above, these follow-on cases are likely to be filed after the investigation is brought to light, either when announcing a settlement or during interim statements made about an investigation.

---

[27] Indeed, agencies are often directed to consider how to coordinate parallel proceedings intra- and inter-agency. *See* 12 U.S.C. § 5515 (2018) (requiring the Consumer Financial Protection Bureau to coordinate investigations and enforcement actions with other agencies); Dep't of Just., *U.S. Attorneys' Org. and Functions Manual* § 27 (Jan. 2012); Sec. Exch. Comm'n, *Enforcement Manual* § 5.2.1 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

[28] Fed. R. Crim. P. 6(e)(2)(B); 31 U.S.C. § 3733(b)(1)(A) (2018).

[29] *See, e.g.*, Compl., *Moore v. Groeb Farms, Inc.*, 1:13-CV-02905 (N.D. Ill. filed Apr. 17, 2013) (filing for bankruptcy after follow-on civil litigation exacted treble damages from the company).

PRACTICE TIP:
FOCUS ON THE RISK OF FOLLOW-ON SECURITIES LAW SUITS

On top of the civil litigation risk relating to the misconduct itself, public companies also face another risk of litigation under the securities laws. Because public companies have certain disclosure obligations in their filings and statements, any material misstatement or omission contained in those statements can be an independent basis for suit. Thus, a company could face regulatory scrutiny and civil litigation about its conduct, coupled with an additional independent suit about its statements concerning that conduct before or during the investigations. Too much disclosure could be inaccurate and could also create unnecessary regulatory momentum and become a self-fulfilling prophecy. On the other hand, too little disclosure or inaccurate disclosure could expose the company to litigation risk (and criticism from investors) when a resolution is ultimately announced. To avoid this, be sure to comply with the regulatory disclosure requirements and ensure that the lawyers work closely with the public relations team handling the messaging during the crisis.[30]

Responding to Legislative Action

If the company crisis is big enough or sufficiently in the public eye, it is possible that there will be legislative action or administrative rulemaking aimed at addressing similar conduct in the future. In especially major cases, Congress may engage in its own investigation, subpoenaing witnesses and documents.[31]

How to handle a congressional investigation is a topic of its own, fit for its own book. But, as they relate to regulatory investigations and prosecutions, congressional investigations can present their own host of issues. A witness's testimony—whether at a public hearing or in a private session with staffers—will help set the factual record that the regulator will also consider. An insufficiently prepared witness can also be lulled into making statements that are insufficiently complete or untrue, undermining that witness's credibility in the regulatory matter and potentially subjecting the witness to prosecution for the untruth. Publicity can add fuel to the fire of a regulatory investigation, putting pressure on the regulator to aggressively

[30] Public relations and message management are discussed in further detail in Chapter VIII: Public Relations & Message Management.

[31] Michael L. Koempel, Cong. Research Serv., *A Survey of House and Senate Committee Rules on Subpoenas* (2017), https://fas.org/sgp/crs/misc/R44247.pdf.

charge a violation. In addition, a company should assume that documents produced in a congressional investigation will also have to be produced to regulators or will be made public by the congressional committee itself, potentially even putting the privilege at risk.[32]

CASE STUDY: CONGRESSIONAL RESPONSE TO THE WELLS FARGO SALES SCANDAL

In September of 2016, Wells Fargo was fined $185 million to settle accusations that its employees created two million fake accounts, which catalyzed customer charges and hurt credit scores, to satisfy sales pressure coming from the top-down.[33] Later, Senator Sherrod Brown, the Senate Banking Committee's top Democrat, and Representative Brad Sherman introduced a bill that would allow victims of the Wells Fargo scandal (and similar scandals) the opportunity to sue, rather than have their disputes arbitrated as required by contract.[34] For its part, Wells Fargo disputed the applicability of the clauses and ultimately settled with civil plaintiffs rather than forcing the arbitration clause issue.[35]

When Congress is considering taking legislative action in response to a crisis, it is important to stay engaged in this process to best provide relevant input on what action is necessary and how to effectuate it. If there is a danger of over-correction, emphasize the limited scope of what caused the problem in order to ensure that any legislative or administrative action has as narrow a focus as possible. To maintain credibility in the public sphere while debating this possibility, it will be important to be viewed as cooperating and immediately fixing any known issues. If the public views this as an isolated incident that is being fixed, Congress may be less likely to respond with negative legislative action. Even in instances where legislative or administrative action is warranted, having a voice in what those changes need to be may be useful in any remaining pending investigations or civil litigation.

---

[32] For a fuller discussion of the privilege in Congressional investigations, *see* Chapter V: Data Privacy & Blocking Statutes.

[33] Press Release, Consumer Fin. Protection Bureau, *Consumer Financial Protection Bureau Fines Wells Fargo $100 Million for Widespread Illegal Practice of Secretly Opening Unauthorized Accounts* (Sept. 8, 2016), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-fines-wells-fargo-100-million-widespread-illegal-practice-secretly-opening-unauthorized-accounts/.

[34] Justice for Victims of Fraud Act, S. 552, 115th Cong. (2017).

[35] Press Release, Wells Fargo, *Wells Fargo Announces Agreement in Principle to Settle Class Action Lawsuit Regarding Retail Sales Practices* (Mar. 28, 2017), https://www.wellsfargo.com/about/press/2017/class-action_0328/.

Finally, remember that public comments about any impending rules will be considered by any regulators still investigating the conduct and by investors considering securities suits.[36]

Beginning in the earliest phases of a multi-jurisdictional crisis, a company must engage in a rigorous analysis directed at identifying the potential downstream consequences of attendant investigations and actions. This process can be used to articulate priorities and goals, to which the company should then refer throughout the process of crisis management, from responding to initial requests to negotiating final settlements. Planning in this way can reduce the costs associated with the crisis and limit disruption of the company's business activities, thereby minimizing the ultimate impact of the crisis on the company.

[36] Public statements are discussed in further detail in Chapter VIII: Public Relations & Message Management.

Checklists

Introduction

On the pages that follow, we have included a number checklists. These are designed to be keyed to particular and recurring phases of crisis management and incident response, including:

1. Scoping an investigation.
2. Building a Team.
3. Producing Documents & Information.
4. Conducting Interviews.
5. Interacting with Authorities.
6. Speaking to the Media.
7. Taking Adverse Personnel Action.

Each checklist is cross-referenced to the relevant substantive chapters of the Handbook, and designed to help you quickly think through and identify information that may be necessary for the task at hand.

Checklist 1: Scoping an Investigation

✓ **Assess what is known about the subject matter, including how the company became aware of it.**

Chapter I: Managing The First Response
Chapter III: Conducting an Internal Investigation
Chapter VI: Employee Rights and Privileges

✓ **Establish the investigation's goals.**

Chapter III: Conducting an Internal Investigation

✓ **Determine the custodians likely to have relevant information and the location of documents and electronic data.**

Chapter I: Managing The First Response
Chapter III: Conducting an Internal Investigation
Chapter V: Data Privacy & Blocking Statutes

✓ **Prepare an investigative plan.**

Chapter III: Conducting an Internal Investigation

✓ **Brief relevant stakeholders on progress.**

Chapter I: Managing The First Response
Chapter II: Responding to Requests From Authorities
Chapter III: Conducting an Internal Investigation

✓ **Decide whether remediation is appropriate.**

Chapter III: Conducting an Internal Investigation
Chapter VII: Cooperation
Chapter IX: Collateral Considerations

✓ **Consider whether, and how, to disclose investigation's findings.**

Chapter III: Conducting an Internal Investigation
Chapter VII: Cooperation
Chapter VIII: Public Relations & Message Management
Chapter IX: Collateral Considerations

Checklist 2: Assembling a Team

✓ **Determine whether the matter is best handled by in-house or outside counsel.**

Chapter I: Managing The First Response
Chapter III: Conducting an Internal Investigation
Chapter IV: Preserving Legal Privilege
Chapter VIII: Public Relations & Message Management

✓ **Assess whether the matter is related to an already-existing investigation.**

Chapter III: Conducting an Internal Investigation

✓ **Assess what subject-matter expertise is likely necessary.**

Chapter I: Managing The First Response

✓ **Assess where the evidence is located and whether expertise is necessary in different jurisdictions.**

Chapter I: Managing The First Response
Chapter V: Data Privacy & Blocking Statutes

✓ **Identify the relevant stakeholders.**

Chapter I: Managing The First Response
Chapter III: Conducting an Internal Investigation

✓ **Establish a mechanism for reporting up and information sharing.**

Chapter III: Conducting an Internal Investigation

Checklist 3: Producing Documents & Information

✓ **Determine whether the request is within the sending authority's jurisdiction.**

Chapter II: Responding to Requests From Authorities

✓ **Assess legal impediments to complying with the request.**

Chapter II: Responding to Requests From Authorities
Chapter V: Data Privacy & Blocking Statutes
Chapter VI: Employee Rights and Privileges

✓ **Decide when and how to produce and negotiate the scope and timing of the requested information.**

Chapter II: Responding to Requests From Authorities

✓ **Determine likely custodians and other sources of data and secure the evidence.**

Chapter I: Managing The First Response
Chapter III: Conducting an Internal Investigation

✓ **Circulate, and update, a litigation hold notice.**

Chapter IV: Preserving Legal Privilege

✓ **Determine the best means of conveying the requested information.**

Chapter II: Responding to Requests From Authorities
Chapter IV: Preserving Legal Privilege

✓ **Assess collateral consequences of producing requested material.**

Chapter II: Responding to Requests From Authorities
Chapter VII: Cooperation
Chapter IX: Collateral Considerations

Checklist 4: Conducting Interviews

✓ **Assess potential legal restrictions on conducting interviews.**
Chapter VI: Employee Rights and Privileges
Chapter V: Data Privacy & Blocking Statutes

✓ **Determine whether the individual requires separate counsel.**
Chapter III: Conducting an Internal Investigation

✓ **Assess how the interview should be documented, including an analysis of the risk of disclosure in applicable jurisdictions.**
Chapter IV: Preserving Legal Privilege

✓ **Determine who should attend the interview.**
Chapter IV: Preserving Legal Privilege

✓ **Assess whether to provide the interviewee with topics or relevant documents in advance of the interview.**
Chapter III: Conducting an Internal Investigation

✓ **Evaluate how to disclose the interview to relevant stakeholders, including internally and to relevant enforcement authorities.**
Chapter VII: Cooperation
Chapter VIII: Public Relations & Message Management

Checklist 5: Interacting With Authorities

✓ **Assess the subject-matter and scope of authorities' interest and jurisdiction.**

Chapter I: Managing The First Response
Chapter II: Responding to Requests From Authorities

✓ **Assess whether the requested information implicates similar requests from other authorities.**

Chapter II: Responding to Requests From Authorities
Chapter III: Conducting an Internal Investigation

✓ **Negotiate a schedule for relevant events.**

Chapter II: Responding to Requests From Authorities

✓ **Keep authorities apprised of developments, to the extent appropriate.**

Chapter II: Responding to Requests From Authorities
Chapter VII: Cooperation

✓ **Determine whether to report findings of internal investigation to authorities.**

Chapter IV: Preserving Legal Privilege
Chapter VII: Cooperation

Checklist 6: Speaking to the Media

✓ **Consider whether to hire a public relations firm.**
Chapter VIII: Public Relations & Message Management

✓ **Coordinate all disclosures with advice of counsel.**
Chapter VIII: Public Relations & Message Management
Chapter IV: Preserving Legal Privilege

✓ **Coordinate messaging with relevant stakeholders.**
Chapter VII: Cooperation
Chapter VIII: Public Relations & Message Management

✓ **Assess the effects of disclosures on ongoing matters as well as potential future litigations.**
Chapter VIII: Public Relations & Message Management
Chapter IX: Collateral Considerations

✓ **Assess legal duties to make public disclosures.**
Chapter VIII: Public Relations & Message Management
Chapter IX: Collateral Considerations

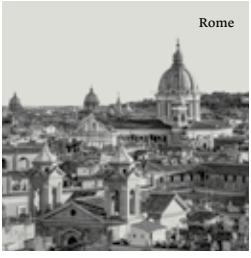
Checklist 7: Taking Adverse Personnel Action

- ✓ **Maintain timely and thorough personnel files, including by conducting regular performance evaluations with written documentation, and record negative performance issues as they occur.**
  Chapter VI: Employee Rights and Privileges

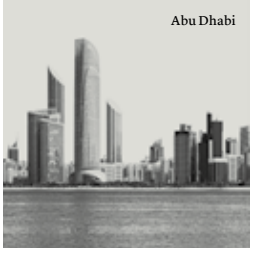
- ✓ **Carefully document the proper justifications for an employee's termination and be prepared to defend those justifications in follow-on legal proceedings.**
  Chapter VI: Employee Rights and Privileges

- ✓ **Create a clear record demonstrating that the discipline is unrelated to any whistleblowing activity.**
  Chapter VI: Employee Rights and Privileges

- ✓ **Ensure that senior management is well-trained and committed to compliance with the securities laws and that clear procedures are in place to report, investigate, and take appropriate action when made aware of potential violations of law.**
  Chapter VI: Employee Rights and Privileges



CLEARY GOTTLIEB



clearygottlieb.com

18.060402_081318