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.