InfoPAK™

Crisis Management in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in a Global Environment

Sponsored by:

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates
Corporate crises, by their very nature, can severely disrupt a company and jeopardize its future. Effective management of the crisis is essential to minimizing disruptions to a company’s ongoing operations, protecting its brand and image, and ensuring its overall survival. This InfoPAK℠ addresses a wide range of issues that commonly arise when a crisis hits, such as media relations, document preservation requirements, international issues, communications with authorities, public disclosure obligations, and data privacy, employee and human resources considerations. It also offers practical tips to in-house counsel with respect to both preparing for and handling a crisis.

The information in this InfoPAK℠ should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Skadden, Arps, Slate, Meagher & Flom LLP or of ACC or any of its lawyers, unless so stated. Further, this InfoPAK℠ is not intended as a definitive statement on the subject and should not be construed as legal advice. Rather, this InfoPAK℠ is intended to serve as a tool for readers, providing practical information to the in-house practitioner.

This material was compiled by Skadden, Arps, Slate, Meagher & Flom LLP. For more information about Skadden, please visit their website at http://www.skadden.com or see the “About the Author” section of this document.

The ACC wishes to thank the members of the Litigation Committee for their contributions to the development of this InfoPAK℠.
Contents

I. Introduction .......................................................................................................................... 5

II. Preparing for and Managing the Crisis ............................................................................ 8
    A. Crisis Management Plan .............................................................................................. 8
    B. Preliminary Steps for Managing a Crisis ...................................................................... 9
    C. Step-By-Step Crisis Management ............................................................................. 11

III. Dealing with the Media .................................................................................................. 12
    A. Media Relations Plan ................................................................................................ 12
    B. Strategic Considerations .......................................................................................... 16
    C. Special Concerns Regarding Sensitive Information Provided to Public Relations Professionals ... 18

IV. Preserving Documents .................................................................................................... 20
    A. When the Duty to Preserve Arises .......................................................................... 20
    B. Content and Dissemination of a Document Preservation Directive ....................... 22
    C. Practical Considerations and Suggestions for Compliance .................................... 23

V. Considering the International Dimensions of a Crisis ................................................... 26
    A. Legal Obstacles to Foreign Document Discovery .................................................. 26
    B. Cultural Differences ................................................................................................. 31
    C. Privilege .................................................................................................................. 31

VI. Interacting with Insurers and Auditors ......................................................................... 33
    A. Insurance Coverage .................................................................................................. 33
    B. Independent Auditors .............................................................................................. 34

VII. Communicating with the Government ......................................................................... 39
    A. Knowing the Company’s Regulators and Enforcement Authorities ....................... 39
    B. Cooperating with Government Entities ................................................................... 41
    C. Reporting to Government Entities ........................................................................... 44

VIII. Meeting the Company’s Public Disclosure Obligations ............................................. 46
    A. Regulatory Provisions Bearing on Disclosure ...................................................... 46
    B. Duty to Disclose in Special Circumstances ............................................................. 48
    C. Voluntary Disclosure .............................................................................................. 48
I. Introduction

The last several years have seen major events around the world impacting companies in the automobile, health care and medicine, security and cybersecurity, oil and gas, travel, banking, and even sports and entertainment industries. These events have occurred around the globe, from outbreaks of serious viruses in West Africa and Latin America; to massive earthquakes in Haiti, Chile, China and Japan; to terrorist attacks in Boston, Paris, Benghazi and other major cities; to allegations of fraud in vehicle emissions controls in Germany; to massive data breaches in the United States; to the killing of the most wanted terrorist in history in Pakistan; to allegations of bribery by the world’s largest retailer in Mexico:

- 30 current and former executives, officials, and marketing associates of the organization that presides over the most-watched sporting event in the world—including its recently reelected president and his likely successor—were indicted in United States federal court on charges of bribery and allegations that systemic corruption pervaded all aspects of the organization’s worldwide dealings.1

- Data breaches targeted 781 companies in the United States in 2015, following a year in which large data theft incidents occurred at major retailers, restaurant chains, casinos, government offices, banks, and a leading electronics company; even before 2015 began, some 30 million patients had already been the victims of data breaches at health care organizations.2

- A widely celebrated laboratory medical testing startup, valued at $9 billion, voided two years of testing results it had made using the novel testing technology on which it based its business, admitting that the technology failed to meet the company’s own accuracy standards after a series of investigative reports into the company’s practices.3

- Highway testing revealed that numerous automobile models made by one of the world’s three largest auto manufacturers included a system designed to conceal emissions dozens of times in excess of legal limits, resulting in a recall of 11 million vehicles worldwide and a precipitous loss of the company’s market share.4

- The second-largest Asian-based international airline experienced sudden and dramatic losses in stock value and was de-listed from public exchanges after one of its flights disappeared over the Pacific Ocean and a second of its planes was struck by a missile over a conflict zone, both within a matter of months.5

- A retailer among the top 25 largest brands in the world with a market capitalization in excess of $260 billion was the subject of a report alleging a campaign of bribery in its Mexican branch; the board of directors, which had previously dismissed its audit committee’s findings, enacted a 72-point compliance plan in response to the allegations, and a subsequent governmental investigation found no significant wrongdoing—although the company reportedly spent over $675 million in the United States alone defending the allegations even so.6
Not all corporate crises are of the same magnitude as these notable examples. Smaller, less devastating crises, nevertheless, can threaten even the most stable corporations. Whether the crisis is a mass disaster, a product defect, a financial scandal, a cyberattack or data breach, illegal activity by company employees, the arrest of a key executive, or even rumors about the health of a company’s founder and leading innovator, a company’s survival will depend on its ability to manage its affairs during the most chaotic of times.

Although all companies hope that they never have to deal with crises like these, bad things do happen. They happen to good companies; they happen to good people; and they happen, often, without warning.

Different types of companies, of course, will face different types of crises, but the goals of all companies faced with a crisis are generally the same:

- Protect the public from imminent harm and contain all potential safety risks;
- Protect and salvage the company’s reputation;
- Return to normal business routine as soon as possible;
- Minimize short- and long-term damage to shareholder value; and
- Maintain public credibility without escalating civil and criminal litigation risks.

Companies survive crises through advance planning. They survive crises through an understanding of their legal obligations and a commitment to meeting them. They survive crises through an awareness of the various intersecting tracks they will need to navigate to obtain the best outcome for the company. This InfoPAK™ is intended to provide in-house counsel with insights into how to start planning for a day that every corporate executive hopes will never come, and how to identify the key legal issues, various logistical considerations, and the most common pitfalls he or she may face if that day ever comes. In particular, the InfoPAK™ examines the following:

- Section II of the InfoPAK™ provides a brief overview of the ways in which a company can be prepared to manage a crisis.
- Section III discusses media relations and offers strategic advice for dealing with the media as part of a company’s crisis management plan.
- Section IV describes the document preservation considerations that a company should address to be prepared to respond to the parallel proceedings likely to follow a crisis, including when such obligations arise and how to comply with them.
- Section V addresses international issues that may be implicated for the ever-growing number of companies with global sales, operations or facilities.
- Section VI addresses third-party interactions for which a company should be prepared when a crisis occurs, including communications with its insurance carriers and disclosures to the company’s independent auditors.
- Section VII addresses communications with the government following a crisis.
- Section VIII discusses public disclosure obligations that may be triggered by a crisis.
- Section IX touches generally upon internal investigations, including questions a company should consider before undertaking such an investigation.
- Section X highlights the potential for privilege waivers in the course of the various interactions that flow from a crisis.
- Section XI identifies employee and other human resource considerations that may arise in the wake of a crisis.
II. Preparing for and Managing the Crisis

When a crisis occurs, the most urgent questions that need to be answered are:

- What happened?
- What is the impact?
- What are you doing about it?
- Whose fault is it?
- How can you prevent it from happening again?

The potential repercussions of a mishandled crisis—including premature or inaccurate responses to these questions—are manifest. A company’s reputation may be severely damaged, customers may be lost, the risk of litigation may arise, and government intervention may be unavoidable.

Corporate crises come in various forms, and can begin in numerous ways depending on the industry (or industries) in which a company operates. Among other things, a damaging press report, a congressional or government inquiry, an advocacy group, an atypical disclosure in a public securities filing, or even an internal alert to a certain risk could all trigger a crisis. However, once begun, crises tend to share certain common elements, including a lack of reliable information, loss of control, extensive scrutiny and confrontation from outside forces, and, of course, anxiety and panic. In other words, the normal corporate decision-making process, where decisions are based on reliable and solid information in a calm and deliberate fashion, is turned upside down. In some circumstances, other factors such as a decentralized organization, fragmentation of responsibility, absentee senior management, and the remote location of the crisis site only add to the confusion.

A. Crisis Management Plan

For the reasons stated above, a company should consider developing a crisis management plan. The most effective crisis management plan is generally one that was put in place before the occurrence of the crisis. Such a plan could include:

- Identification of areas where the company might be vulnerable to crisis;
- A compliance program designed to identify fault lines in the company’s operation that might give the company an early warning of a pending crisis;
- Distribution of emergency contact numbers among senior managers to facilitate contact should a crisis hit;
- Delegation of a crisis management team (see section II.B) and clear division of crisis-related responsibilities between its members;
- Designation of outside legal counsel and outside public relations specialists to consult in case of crisis;
Preparation of template statements for use in a crisis; and
Issuance of a crisis manual.

After a crisis management plan is prepared, organizations also should ensure that the plan remains current. Any written components of the crisis management plan, such as the crisis manual, contact information, and any related policies and procedures, should be reviewed and updated at least annually. To remain prepared, organizations also should conduct regular exercises among the crisis management team at least annually to test its reactions to unexpected news of a crisis. Feedback from the exercises should be shared with the team members to better prepare them for potential future crises.

Taking these steps before a crisis occurs and tasking individuals with particular responsibilities when something goes wrong should ease anxiety and panic and facilitate more reasoned judgments and decisions.

In addition to a general crisis management plan, given the proliferation of cybersecurity events in recent years and the potentially devastating impact they can have, organizations should consider designing a crisis management plan targeted specifically at the occurrence of a cyber breach or crisis. Although this plan should include the items listed immediately above, the creation of a cyber crisis plan also may include making assessments regarding the type of data a company is seeking to protect, the costs associated with that protection, and the relevant statutes and regulations – specifically, various state breach notification laws.

In September 2015, the U.S. Securities and Exchange Commission (SEC) issued a risk alert release announcing that the Office of Compliance Inspections and Examinations (“OCIE”) will be conducting a new Cybersecurity Examination Initiative whereby the OCIE will evaluate registered broker-dealers and investment advisers’ various cybersecurity-related controls and test implementation of those controls. Further to this point, in September 2016, a proposed new regulation in New York — to go into effect January 1, 2017 — would require banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services to establish and maintain a cybersecurity program. Some key requirements of this new regulation include: (i) creation of a cybersecurity policy; (ii) appointment of a chief information security officer; (iii) yearly penetration testing and vulnerability assessments; (iv) employment of cybersecurity personnel; (v) implementation of written vendor policies; and (vi) creation of a cyberattack incident response plan. Given the increasingly heightened interest in cybersecurity controls by U.S. federal and state regulators, it would be prudent for companies across all industries to design, adopt, and continually test and update cyberattack response plans.

B. Preliminary Steps for Managing a Crisis

Even where a company in crisis does not have a pre-existing crisis management plan, a company can take immediate actions to assist it in managing the crisis.

First, the company should set up a crisis management team. Depending on the particular circumstances of the crisis at hand, this team should be composed of, if appropriate:

- A senior officer, such as the CEO, the president, the COO, or the CFO;
Senior members of the legal, compliance, public relations, security, finance, marketing, risk management, government relations and/or human resources departments;

Outside technical advisors such as scientific experts, environmental clean-up specialists, cybersecurity experts, or forensic accountants;

Outside public relations specialists; and

Outside legal counsel.

The composition of the crisis management team should be tailored to the particular nature of the crisis, as necessary. For example, if the crisis involves allegations of financial improprieties by senior officers of the company, the company may need to exclude such individuals from the crisis management team and to look, instead, to members of the board of directors to serve as the senior members of the team. To help minimize the occurrence of cybersecurity crises—if feasible—hiring an internal chief information security officer (“CISO”) should be considered. In this instance, in-house counsel would work closely with the CISO in developing, executing, and modifying the data breach or cyber crisis management plan.

It is very important that members of the team work together closely and cooperatively. A course of action may be viewed very differently by the different disciplines brought together to address the crisis. For example, actions that make sense from an operations perspective, such as the deployment of a large number of employees to a particular location, may not make sense from a human resources perspective. And actions that may be prudent from a legal perspective, such as silence in the face of media inquiries, could result in a public relations disaster.

Second, the company should appoint a single high-level spokesperson to address issues relating to the crisis. This demonstrates to third parties that the company is appropriately concerned about the crisis and is taking the matter seriously. It also permits the company to speak through a single voice. The spokesperson should join the crisis management team, if he or she is not already a member of it when appointed—for example, in many situations, consumers may expect the CEO to speak for the company in times of crisis.

Third, the company should determine the specific roles of key executives and identify clear lines of responsibility. Doing so will ensure that all bases are covered and that nothing is left unattended.

Finally, the company should establish protocols for notifications and internal communications to ensure that information is appropriately communicated to those with a need to know. If the company maintains social media accounts, these protocols also should strictly oversee what material may be posted to those accounts.

Although it may be difficult to address each of these administrative tasks in the midst of a crisis, proceeding without a crisis management team could prove disastrous. A company in crisis should resist the urge to simply respond to the pressing demands of the crisis in an ad hoc, uncoordinated manner (except, of course, when an immediate response is necessary; for example, to protect the public). If the company has a pre-existing crisis management plan, it should follow it. If the company does not have such a plan, it should move swiftly to establish a crisis management team.
C. Step-By-Step Crisis Management

Organizations should be prepared to respond quickly and effectively to a crisis. Although every crisis is different, an organization’s initial response to a crisis should generally include the following basic elements.

In the first hour after the company recognizes a crisis:

- Arrange a meeting of the crisis management team to be convened within 24 hours.
- If the crisis involves physical danger, ascertain the scope of the danger and ensure company personnel are or will be in control of the crisis and that appropriate law enforcement agencies are informed.
- Develop a response to potential media inquiries during the first 24 hours of the crisis; this response could offer no comment on the crisis but promise a future update (a template response may be scripted in the crisis management plan) or indicate that the organization is aware of the issue and would comment at the appropriate time. The crisis management team should be careful not to overpromise or make statements that cannot later be supported or, worse, could be inaccurate.
- Contact outside technical advisors, public relations specialists, and legal counsel to advise them of the situation and obtain support as needed.

Within the first 24 hours after a crisis occurs:

- Convene the crisis management team, including outside advisors.
- Designate a high-level spokesperson for the company.
- Clearly establish the responsibilities of each member of the crisis management team (these responsibilities may be listed in the crisis management plan).
- Prepare initial public statements and releases on the crisis (draft statement templates may be scripted in the crisis management plan).
- Establish protocols for gathering information, ensuring safety, conducting internal investigations, releasing public statements, monitoring social media, and taking other action moving forward, making sure to provide for regular contact between members of the crisis management team (standard protocols may be written in the crisis management plan).

Thereafter, ensure that the protocols set in the crisis management plan, or in the first 24 hours of the crisis, are followed, but remain flexible. The crisis management team should continue to meet regularly to discuss the crisis until the company is satisfied that it has passed. Indeed, rushing an action plan or scrambling to pull team members together only after an incident occurs will dramatically increase the risk of mishandling a crisis. Attached as Appendices A and B to this publication are “checklists” that might be useful in (a) identifying procedural considerations in responding to a crisis and (b) recognizing what issues might involve legal implications and the prudence in retaining competent counsel in relevant jurisdictions.
III. Dealing with the Media

In today’s media-saturated environment, a company in crisis is likely to be subject to immediate, constant and intrusive media scrutiny. The aspects of a corporate profile that a company normally might tout (size, profitability, reputation for quality and integrity) may well be the lightning rod for negative press when misfeasance or malfeasance is alleged. Aside from generic news stories about corporate greed or bloated executive compensation, companies can expect public interest to be piqued by allegations of fraud or corruption, environmental disasters, data breaches, trading with enemy states and serious public health violations—just to name a few.

Given the prevalence of social media and the instant availability of news media, including everything from journalists’ tweets to breaking news updates on the New York Times app, a company in crisis must confront a critical question almost immediately: how to deal with the media. Gone are the days when companies and their lawyers can reflexively respond to press inquiries with “No comment.” Lawyers may wish to limit the company’s legal exposure by instituting a media blackout, but in today’s world, the public frequently interprets silence in the face of pointed allegations as an admission of guilt. Faced with this reality, companies often conclude that the reputational risk of saying nothing outweighs the legal risk of defending itself in the court of public opinion.

Typically, time is of the essence when dealing with the media in crisis situations, but the timing of media announcements may be influenced by statutory or regulatory regimes relating to the focus of the crisis. For example, a company may have a strong desire for immediate disclosure of cyber events, particularly when a data breach involves the compromise of personal information that could lead to reputational harm, public mistrust, litigation and government investigations. Although no U.S. federal laws currently govern when companies are required to notify the public of a data breach, nearly every state has enacted data breach notification requirements of varying forms. Moreover, industry-specific notification requirements and international notification obligations may influence when a company notifies the media of such a breach.

Parallel proceedings add a dimension of complexity that must be considered when developing a media strategy. Public statements intended to protect the company’s reputation and ease investor concerns at the outset of an investigation may have unanticipated consequences later when the company responds to insurers, state and federal criminal investigations, regulatory inquiries, congressional hearings, inquests of interested foreign governmental authorities and international organizations and class-action and securities litigation. If the company decides that it has little choice but to respond to the media and directly address allegations of malfeasance, it should consider several basic guidelines before issuing its first press release or agreeing to its first interview.

A. Media Relations Plan

Today’s media moves at record speed. Ideally, then, a crisis management plan should involve preemptive steps that can mitigate the fallout from a public relations crisis. While each crisis is unique, a company should have a media relations strategy that seeks to
identify and resolve potential issues before they develop into a full-blown crisis. A company also should consider creating a checklist of steps that need to be taken to ensure that a media relations plan is formulated and executed properly. The media relations plan should address, at a minimum, the following topics:

1. **Appoint an Experienced Spokesperson**

   As noted in Section II, a crucial part of any crisis management plan is the identification of an experienced, high-level spokesperson to interact with the press and other relevant third parties. This spokesperson should have the requisite skills to interact with the media. He or she must respond promptly to all media inquiries and respect reporters’ deadlines, even when the company is not in a position to provide much information. Reporters are human and can take umbrage if they feel they are being ignored. A company should do what it can to prevent any perceived slights from negatively influencing a reporter’s story.

   Although the spokesperson preferably should hold a senior position at the company and be part of the crisis management team, it is not necessary that the CEO serve as the spokesperson. In fact, there may be circumstances where the CEO should not serve as the spokesperson. For example, there may be a question as to the CEO’s role in the crisis, or the CEO’s involvement, by itself, could lead to negative media coverage (e.g., if the CEO has been the subject of recent negative media coverage). It also may be more appropriate for a lower-level executive to serve as the spokesperson rather than the CEO. In some circumstances, the involvement of the CEO could give undue weight to an issue and inadvertently create a larger media crisis. It also may be prudent to keep the CEO free to focus on fulfilling his or her crisis management responsibilities, or to reserve the CEO to make public statements when the facts of the crisis and the company’s response thereto are known. Regardless of the spokesperson’s rank, he or she must have direct and regular contact with the crisis management team to ensure that, to the extent the company determines that disclosures to the media are appropriate, the spokesperson is conveying accurate and up-to-date information.

2. **Funnel All Inquiries and Communications Through the Crisis Management Team**

   The crisis management team needs to serve as the clearinghouse for all of the company’s public pronouncements regarding the crisis, including, but not limited to, press statements, congressional testimony, governmental filings and even internal companywide communications to employees about the crisis. The team needs to oversee and coordinate all such crisis-related statements to ensure that inconsistent messages and positions are not communicated publicly or internally. The spokesperson and his or her support staff need to be an integral part of the process in order to avoid missteps with the media.

   The company also should make clear to employees that all press inquiries must be referred to the appropriate public relations personnel. Similarly, they must be cautioned that “off-the-record” and “not-for-attribution” conversations are fraught with danger, as even scrupulous journalists have different understandings of how such comments can be used. Employees also should be reminded as soon as possible to refrain from voluntarily commenting on the crisis, including in conversations, emails, text messages, social media,
internet comment boards, and blogs. Public comments by employees—especially those not knowledgeable about the facts or the company’s overarching media strategy—can spark a media frenzy, provoke regulators and prosecutors, and provide fodder for plaintiffs' counsel.

The crisis management team also should coordinate efforts to investigate and remediate the crisis. From a communications perspective, this may involve managing internal systems to ensure that information is not unintentionally leaked (for example, by a whistleblower or a careless employee). Email freezes may be appropriate under certain circumstances to ensure that unintended information leaks do not occur and that all communications with the media are properly considered by, and channeled through, the crisis management team.

3. Understand the Company’s Disclosure Obligations

There is a close and reciprocal relationship between a public company’s disclosure obligations and its media relations plan. As developed more fully in Section VII, public companies are subject to a variety of laws and regulations governing disclosure of material non-public information to the investing public. The SEC, other regulatory agencies and governmental contract partners, as well as private entities such as banks and insurance companies, may require some form of disclosure of material liabilities. At the same time, any public disclosure of potential liabilities is likely to stimulate further media inquiries. A company’s media relations plan should be coordinated closely with its investor relations department and disclosure counsel. As noted above, providing a consistent message in all public statements and disclosures is critical to minimizing negative media impact in a crisis.19

Cyber threats and breaches present unique disclosure complications. In fact, the SEC has issued guidance regarding disclosure obligations with respect to cybersecurity risks and cyber incidents.20 Furthermore, as highlighted above, companies may have to adhere to specific state and industry breach notification requirements related to data breaches. For those companies facing cyber and data security risks, senior leadership should ensure that the media relations plan is aligned with the company’s cyber disclosure obligations.

4. Identify and Cultivate Key Media Contacts

Due to the unfortunate realities of corporate crises, much of a company’s contact with the media during the earliest stages of an emergency likely will be reactive. When trying to develop a media strategy in the throes of a crisis, company public relations personnel usually will spend most, if not all, of their time deciding whether to respond to media inquiries and what should be communicated in response to such questions.

If the company decides, however, that proactively engaging the media is in its interests and feasible, it will need to know which media outlets and reporters it should approach to get ahead of the story and effectively communicate the company’s message. The media relations team should research media outlets ahead of time and look to incorporate the following into the company’s media relations plan:

- Media outlets inclined to give the company a fair hearing;
For more ACC InfoPAKs, please visit http://www.acc.com/infopaks

- Journalists already knowledgeable about the company;
- Columnists and editorialists sympathetic to the company’s mission;
- Trade press with the technical expertise to grasp the nuanced issues facing the company and its industry; and
- Blogs and online sources that are likely to focus on the company’s business.

Attempting to develop this basic intelligence on the fly, rather than researching it ahead of time, likely will cause the company to stay one step behind the story. Information can be reported broadly within a matter of minutes, making it crucial to keep pace with the speed of today’s news reporting.

5. **Prepare a Social Media Strategy**

A company can no longer ignore the importance of Twitter, Facebook, Instagram, and other forms of social media. An effective use of social media can help mitigate potential damage from a crisis, while conversely, poor use of social media can throw fuel on a fire and intensify a media crisis. Having a social media plan in place is thus an essential component of an effective media relations plan. Some of the key issues that a social media strategy should address include the following:

- Monitoring social media—A company must be aware of blogs, online sources (like dedicated websites), and social media that are likely to focus on the company’s business. When a crisis breaks—and ideally, beforehand—the crisis management team must monitor these sources to understand the public’s understanding of and reaction to the crisis.

- Controlling social media—When confronted with a crisis, a company needs to understand what social media it uses and how to control it. For example, some companies have scheduled social media postings. When a crisis breaks, a company should consider freezing all scheduled postings until it knows the full scope of an issue. Without a freeze, a company may find that its social media posts inadvertently bear on the issue(s) involved in a crisis. As previously indicated, maintaining a consistent message is key, and social media postings must be a part of that consistent message.

- Proactive use of social media—Twitter, Facebook, and a number of other social media platforms can be used to inform and mobilize key constituencies. A crisis management team should be particularly keen to turn to social media to advance its message.

- Indirect use of social media—The company can indirectly use social media by communicating with relevant bloggers or journalists active on social media who might be more inclined to spread the company’s message.

- Search engine results—A company should consider taking the preemptive step of optimizing search engine results so that the company’s website and social media outlets—and by extension, the company’s message about a crisis—appear first on search engine landing pages.

Note, however, that any use of social media must be carefully thought out. Such actions as deleting social media posts, arguing with social media users, and diluting the company’s
message through extensive use of social media could lead to any number of negative consequences during a media crisis and should be avoided.

B. Strategic Considerations

In addition to developing a media relations plan, the company also should pay particular attention to the timing of voluntary statements, the content of its statements, how to effectively disseminate those statements and the effect those statements are likely to have on the anticipated audience.

1. Carefully Time Voluntary Statements

The timing of a company’s announcement about its response to a negative event, including the decision to conduct an internal investigation, is one of the earliest and most critical decisions a company will have to make during this process. Public relations personnel likely will want to respond as promptly as possible to shape the media’s coverage and the public’s perception of the crisis. Lawyers, however, typically prefer to wait until sufficient facts are gathered before publicly announcing a strategic response and/or investigation.

In high-profile corporate crises, a company does not have the luxury of time. Generally, the company’s safest course of action will be to issue a public statement as soon as possible after the company learns about the crisis and launches its own internal investigation. A prompt response sends the message that the company is attentive, responsive, and transparent. Waiting too long may leave an impression that the company is covering up wrongdoing or not taking the matter seriously.

2. Craft Messages Positively

The timing of any announcement will, of course, influence the content of the disclosure. It is unlikely that the company or its legal advisers will have sufficient facts, if any, at the outset of a crisis to speak authoritatively about the underlying issues. In such a case, a company should be careful not to make definitive statements about the matter. Committing the company to a position that later proves to be inaccurate can be devastating. Because accuracy is the primary concern, even if a company is not in a position to substantively address the matter (or, as is sometimes the case, the company does not know exactly the origins or scope of the crisis), the company should convey a message that instills confidence in the company and its handling of the matter.

For example, the company could make clear that it is taking the matter seriously, is fully cooperating with government authorities, and is initiating an internal investigation, overseen by the Audit Committee or independent directors, to determine the extent of any problem. Although it is tempting to issue blanket denials of inflammatory allegations, it is generally prudent to resist this temptation because facts gathered during the course of the internal investigation may prove such statements to be inaccurate.
3. Know the Company’s Audiences and Maintain Consistent Messages to All Constituencies

When interacting with the media, the company must keep its target audiences in mind. A company has many constituencies, including employees, shareholders and investors, regulators, insurers, banks, rating agencies, business partners, customers, and suppliers. The company’s communications to its shareholders, of course, must be consistent with its public comments to the press. Employees are a constituency that should not be overlooked. Crises may take a toll on employee morale and productivity. Keeping employees informed will help fend off rumors, speculation, and unnecessary distractions. If the company decides, however, to notify employees of the crisis through a companywide memorandum, assume the memorandum or the information communicated therein will make its way to the media. When preparing such internal communications, remember: Do not put in writing what you would not want to read on the front page of The New York Times.

4. Explore Alternative Online Opportunities, When Appropriate

Assuming the company determines that proactively engaging the news media will, on balance, advance the company’s interests, the crisis management team can investigate alternative methods of communicating its message. A company can establish a separate website dedicated to providing timely, critical information about the crisis to the press and public. If it does so, the company might consider posting carefully vetted fact sheets, FAQs, and videos on the site to inform the press and educate the public. For multinational corporations, translating these materials into multiple languages will facilitate dissemination of the company’s message around the globe. As already noted, the company’s public communications should be consistent with its disclosure obligations and should be made with an understanding that prosecutors, regulators, and congressional staff will read them. Conveying misleading facts or an inappropriate tone likely will alienate or provoke these important constituencies.

Depending on the nature of the crisis and the availability of resources, the crisis management team might consider establishing a “truth squad” or “rapid response team.” Some presidential campaigns have effectively combated misinformation campaigns waged by opponents and special interest groups by quickly identifying and responding to rumors and half-truths being spread about their candidates. Speed and accuracy are the cornerstones of any successful truth squad or rapid response team.

5. Emphasize Remedial Measures When Releasing Investigatory Findings

If the company decides to publicize the findings of its internal investigation, it should simultaneously release and emphasize all remedial measures adopted by the company to address any problems identified. Doing so will reinforce the company’s message that it is committed to proper business practices and has handled the crisis with the utmost seriousness.

For more ACC InfoPAKs, please visit http://www.acc.com/infopaks
6. **Remember that Settlement Documents with Government Agencies Will Be Released to the Public**

Finally, throughout a crisis and particularly when negotiating a resolution to any government investigation, a company should take into account that non-prosecution agreements, deferred prosecution agreements, injunctions, cease-and-desist orders, consent decrees, corporate integrity agreements, and other dispositions with government agencies typically will be publicly available. The media will consider the statement of facts in such documents to be the definitive account of what actually occurred. A flawlessly executed media strategy could be undone or undermined if the company’s public statements during the course of the investigation conflict with the version of events set forth in the settlement documents. It is therefore imperative that there be active coordination between those managing legal aspects of the crisis and the media relations personnel.

## C. Special Concerns Regarding Sensitive Information Provided to Public Relations Professionals

Finally, companies should be cognizant of certain special concerns relating to the use of outside public relations (“PR”) consultants. Given the complexity of parallel proceedings and the need for coordination among the personnel handling the various proceedings, many corporations hire PR consultants to help protect the company’s public image. PR professionals often work closely with attorneys conducting the internal investigation. Great care should be taken, however, to ensure that the communications among the company, the attorneys, and the PR personnel are protected to the maximum extent possible by the attorney-client privilege and/or work product doctrine. In the United States, the U.S. Court of Appeals for the Sixth Circuit recently acknowledged the practical reality that responding to media inquiries can have legal implications, but in-house counsel should be mindful that courts have issued conflicting opinions on whether communications between attorneys and PR professionals are privileged.

For example, in *Calvin Klein Trademark Trust v. Wachner,* plaintiffs’ attorneys hired a PR firm in anticipation of filing a high-profile civil suit, for the purpose of assisting the lawyers in understanding possible reactions to the litigation, rendering legal advice, and ensuring that media interest in the action was handled responsibly. The court concluded that communications with the PR firm were not protected by the attorney-client privilege, finding that:

(i) the communications themselves generally did not contain or reveal confidential communications made for the purpose of obtaining legal advice; (ii) the PR firm, which had a prior relationship with the plaintiffs, was providing ordinary PR advice; and (iii) there was no justification for broadening the attorney-client privilege to cover functions not “materially different from those that any ordinary public relations firm would have performed if they had been hired directly by [the plaintiffs] (as they also were), instead of by [their] counsel.”23
In contrast, in *In re Copper Market Antitrust Litigation*, the court concluded that communications between a PR firm and the defendant’s lawyers were protected by the attorney-client privilege where the PR firm was serving as the functional equivalent of an in-house PR department of the defendant. The court thus found that the PR firm was part of the “client” and that its communications with the lawyers therefore were cloaked with the attorney-client privilege.

An opinion issued by the U.S. District Court for the Southern District of New York in the Martha Stewart prosecution, *In re Grand Jury Subpoenas*, provides additional guidance on this issue, and remains one of the seminal decisions in this area of the law. Stewart’s attorneys retained a PR firm because “unbalanced and often inaccurate press reports about [Stewart] created a clear risk that the prosecutors and regulators conducting various investigations would feel public pressure to bring some kind of charge against” her. The court concluded that because some of the communications between the PR consultants and defense attorneys “were directed at giving or obtaining legal advice,” not to provide Stewart with general media relations advice, the communications were privileged.

Although the court confined its opinion to the facts of the case, the opinion in *In re Grand Jury Subpoenas* provides useful guidance on how best to protect communications with PR consultants. At a minimum, the company should consider taking the following steps:

- The company’s outside counsel, not the company itself, should retain the PR firm. The engagement letter should state expressly that the PR firm is being retained to provide advice specifically in connection with anticipated litigation.
- Outside counsel should not hire a PR firm previously retained by the company. The PR firm also should not be asked to perform any general media relations functions not related to anticipated litigation.
- Outside counsel should be present for all communications between the company and the PR firm. Counsel should make clear that all such communications are to assist the attorneys in providing legal advice to the company.

Similarly, in-house counsel managing a cybersecurity attack or data breach investigation should consider engaging outside counsel to ensure the investigative process is fully protected under the attorney-client and/or work product privileges. Organizations should be mindful that if the general counsel manages the CISO in the normal course of business, a court could interpret this reporting structure as an ongoing business relationship that does not fall within the attorney-client privilege parameters. To avoid confusion in this respect, the company can remove the CISO from the legal reporting chain and engage outside counsel to manage the investigation.
IV. Preserving Documents

In the aftermath of a crisis, no company will desire to be in the position of having to acknowledge that documents relevant to the crisis were destroyed, regardless of whether such destruction was intentional or the result of the routine operation of an electronic information system. The consequences of failing to preserve relevant documents are serious and could include:

- Loss of credibility with U.S. government regulators, Congress, or the courts;
- Monetary sanctions;
- Obstruction of justice charges; and
- Prejudice in litigation, including entry of judgment against the company or an adverse inference instruction (i.e., an instruction to the jury that it can presume the destroyed documents contained evidence adverse to the company’s position).  

Accordingly, the crisis management team should consider at the earliest stage of the crisis whether it is prudent to preserve relevant documents and the manner by which that action should be communicated to relevant company employees.

Crises present particular difficulties with respect to the issuance of a document preservation directive. For example:

- At the onset of a crisis, it may be difficult to identify the scope of an appropriate preservation directive given the limited information generally available when a crisis hits.
- Depending on the nature of the crisis (e.g., mass disaster, management shakeup), it may be difficult to communicate the need for document preservation to appropriate individuals.
- Company resources necessarily may be devoted to addressing the crisis itself, limiting the resources available to address document preservation.

These complications, however, do not relieve a company of its obligation to preserve documents. Once a company reasonably anticipates litigation or a government investigation, it must implement a document preservation directive to ensure that relevant information is preserved.

This section discusses when a company’s duty to preserve documents arises, the dissemination and content of a document preservation directive, and practical considerations for company counsel faced with implementing a successful preservation directive in the midst of a crisis.

A. When the Duty to Preserve Arises

A company’s obligation to preserve documents can arise from various sources, including common law, statutes, regulations, and court orders. Although a company should have
record retention policies that ensure compliance with U.S. federal and state statutes, regulations and agency rules (such as mandatory retention periods applicable to certain documents generated in the ordinary course of business), additional document preservation obligations arise when a company “reasonably anticipates litigation.”

Determining when a company “reasonably anticipates litigation” can be difficult. It is particularly challenging when a crisis occurs and the repercussions of the crisis remain unknown. Typically, the duty to preserve is triggered when a company has a suspicion or a reason to believe that a wrongful act has occurred or when the company has knowledge of the intentional destruction of documents outside the formal record retention policy. These triggering events often occur prior to the initiation of a formal or informal investigation or the receipt of a written or verbal threat of litigation. Indeed, threats of litigation can come in a variety of forms, any of which can give rise to a preservation obligation. The most obvious are the filing of a lawsuit or the issuance of a subpoena by a government agency. However, threats of litigation can take other, less obvious forms. For example:

- **Demand Letter.** The duty to preserve may arise when a company receives a specific demand letter from an attorney on behalf of a party who threatens litigation.

- **Regulatory Complaint.** The duty to preserve likely will arise when a company learns that a complaint has been filed against it with a regulatory body, such as the U.S. Equal Employment Opportunity Commission (“EEOC”).

- **Media Reports.** If the company is aware of trustworthy media reports describing facts known to the company that suggest that a government investigation is forthcoming, it may be reasonable for the company to anticipate a government investigation.

- **Past Events.** If a company has experience with past events that resulted in litigation or government investigations (e.g., the collapse of a mine, workplace injuries, employment discrimination claims), such prior experience may be deemed sufficient for a company to reasonably anticipate litigation upon the occurrence of a similar event.

In considering whether document preservation is necessary in response to a crisis, a company should assess the situations that typically result in litigation and assess the known facts and circumstances to determine whether the company can reasonably anticipate civil litigation or a government investigation.

Because a court’s analysis of a company’s pre-litigation preservation decisions will be fact-based, and given the lack of specific guidance as to when the duty to preserve arises, a company should approach each situation on a case-by-case basis and conduct a good faith and reasonable assessment of the likelihood of litigation. Company counsel also should be mindful that government investigators, regulators, and private litigants may second-guess the company’s decisions and actions—this especially holds true for the preservation of digital evidence in the context of a cybersecurity attack where the preservation efforts may differ from traditional document preservation processes. Thus, a crisis management plan should take a conservative approach to document preservation obligations and ensure that in-house counsel and other relevant employees are properly trained in this respect.
B. Content and Dissemination of a Document Preservation Directive

Once the duty to preserve has been triggered, a company is expected to retain all existing relevant documents in its possession, custody, or control, as well as any relevant documents created thereafter. Recognizing that companies often are large institutions with numerous employees, courts in the United States have suggested that the duty to preserve extends to employees that are reasonably likely to possess documents relevant to the litigation or investigation. In addition to employees, a company also may have a duty to preserve relevant documents that are in the possession or custody of third parties, such as vendors, consultants and outside counsel, if the company has control over the documents. Courts typically define “control” as the legal right, authority, or practical ability to obtain the documents sought on demand.

Once relevant employees and, if applicable, third parties, are identified, they should be contacted as quickly as possible to identify all potential sources of relevant information, to understand how and where they store such information and to direct them to preserve potentially responsive information. As a company works to identify where employees store relevant information, it should bear in mind that employees are increasingly using personal devices (e.g., laptops and mobile phones) and cloud-based accounts (e.g., email and data storage accounts) for business purposes. Under certain circumstances, a company may have a duty to preserve relevant information on employees’ personal devices and cloud-based accounts. Companies should recognize that the number of employees likely to have relevant information may increase as more information is learned about the crisis. As the crisis unfolds, relevant employees may also depart the company. Companies should collect and preserve relevant documents that these employees possess so that such documents are not lost, deleted, or destroyed when they depart.

Although employees typically are aware of hard copy documents and electronically stored information (“ESI”) that they themselves have generated or received, they may not be familiar with how the company stores such information more generally. Moreover, it may be necessary to suspend the company’s automatic document destruction policies, such as electronic email deletion programs or the routine overwriting of back-up tapes. It is therefore critical to involve the company’s records managers and information technology (“IT”) personnel in the document preservation process. Consequently, the document preservation directive should be communicated in writing to relevant employees as well as to records managers and information technology personnel.

The preservation directive itself should:

- Be easy to follow;
- Identify all steps that an employee must take to preserve relevant information, clearly defining what information should be preserved and how such information should be preserved;
- Describe potential locations of relevant information, such as desktops, laptops, tablets, BlackBerries, mobile phones, PDAs, hand-held wireless devices, hard drives, servers, storage media (e.g., DVDs, CDs, flash or thumb drives), social media accounts, telephone logs, microfilm, microfiche, calendars, date books, appointment books, diaries, and central storage files.
Emphasize the importance of complying with the directive and the potential legal or other consequences of non-compliance; 

Request that employees keep confidential the information conveyed in the directive; and

Include contact information for any individual responsible for answering questions about the directive.

Depending on the circumstances of the case, it also may be prudent for the company to require confirmation of compliance with the preservation directive to verify that the recipients understand their preservation obligations. Moreover, companies with a global reach should consider translating the directive into additional languages to ensure that it is understood by relevant employees. While a preservation directive is in place, the company should consider sending regular reminders of the directive, such as quarterly or semi-annually, to ensure that employees continue to preserve documents. The company also should implement a procedure to provide the preservation directive to relevant employees who join the company after the initial issuance of the directive.

In issuing a preservation directive, the company should be mindful that, if its preservation efforts are challenged, it can elect to proffer certain preservation communications as evidence of the reasonableness and propriety of its actions. Accordingly, if the company decides to protect its preservation communications with the attorney-client privilege by having company counsel issue such communications, it should be aware of the potential for a later privilege waiver as to such communications. If the company decides that such communications should not be treated as confidential attorney-client communications (for example, by having a records custodian issue the directive), it should be aware that the communications may be discoverable irrespective of whether its preservation efforts are at issue.

C. Practical Considerations and Suggestions for Compliance

Below are some practical considerations for company counsel faced with implementing a successful preservation directive in the midst of a crisis.

I. Document the Preservation Protocol

Because the preservation process may be subject to scrutiny as government investigations and litigation unfold, the company should document the decisions made during the course of implementing the preservation directive. A company that has to defend such decisions with respect to multiple proceedings, potentially years after the implementation of the directives, may need to establish, for example:

- The events that the company believed triggered the duty to preserve documents;
- The date the preservation directive was issued;
- The initial scope of information preserved and why the company believed that such scope was appropriate; and
The employees who received the directive and why the company believed such distribution was appropriate.

Documenting this information will aid the company in establishing that it acted reasonably in the face of a challenge to its preservation efforts.

2. **Consider Forensic Collection of Electronic Data**

The company should consider the need to conduct a forensic collection of electronic data, which may be appropriate to recover deleted data that the company knows is relevant to the crisis, or when the company has concerns that key custodians may not comply with their document preservation obligations. The company also might consider whether to retain a third-party computer forensic vendor to help harvest the data. If the company elects to collect data forensically, the company should maintain a chain of custody for all such materials.

3. **Anticipate the Scope of Document Review and Production**

At the document preservation stage, the company should consider the anticipated scope of document review and production that may be expected as the crisis unfolds. An important part of any investigation and litigation response is the production of documents and ESI. Indeed, a lawsuit’s outcome can be influenced by—or even, in the extreme case, determined entirely by—a party’s success or failure in gathering and producing documents to its adversary.

In a crisis, there are likely to be competing demands for resources, short time frames to respond to requests, requests that do not completely overlap, and lack of clarity about the eventual scope and volume of document requests and responses. Accordingly, the most practical approach is to assume that information requests and responses will be broad, and to implement a process that can be expanded or narrowed as the matter develops. Considering these factors at the onset of a crisis will assist the company in properly scoping its preservation obligations and may serve to reduce the overall costs of the review and production process. In particular:

- Consider an electronic processing and review platform that preserves and makes document metadata and other hidden information available for analysis and review.
- Consider a review platform that allows access and review by multiple users in multiple locations.
- Anticipate that multiple parties are likely to demand documents, possibly in different formats. Carefully track and log the review that is performed in response to different requests, and productions that are made to different counterparties.
- If search terms or other methods of narrowing data for review are used, careful records should be maintained of all such steps.
In sum, to ensure compliance with its document preservation obligations and avoid disputes about its preservation efforts, a company that reasonably anticipates litigation should:

- Act quickly to preserve;
- Communicate the duty to preserve with a preservation directive;
- Document a preservation protocol;
- Work with information technology personnel and records managers;
- Avoid destruction of potentially relevant evidence, including by third parties if possible;
- Avoid modifying electronic documents, including metadata, by opening, printing, copying or forwarding original files;
- Consider consulting with third-party computer forensics experts;
- Maintain a chain of custody; and
- Anticipate production demands.
V. Considering the International Dimensions of a Crisis

U.S.-based crises—particularly government investigations and private litigation—are notoriously document intensive. Government enforcement proceedings are driven by subpoenas, voluntary document requests, and civil investigative demands, and civil litigation is fueled by document requests and third-party subpoenas.

When a crisis has an international component—through the involvement of a foreign litigant, prosecutor or regulator, or because the company has documents located overseas—document gathering and production are even more complicated. This is because there is no uniform set of rules that governs cross-border discovery. Rather, cross-border discovery is governed by a patchwork of the laws, regulations, court rules, and local customs of the jurisdictions with an interest either in the proceeding or in the documents at issue. Moreover, the requirements of the various jurisdictions in which a company does business often conflict, raising questions about how the company can comply with all its different obligations.

In light of these complications, the crisis management team of a company involved in cross-border discovery must think globally and look to local experts for advice and guidance. The use of local experts will help the company comply with its legal obligations in each jurisdiction. Oversight by the crisis management team will ensure that the company’s compliance with one jurisdiction’s requirements does not affect its rights against parties in another.

This section discusses three issues a crisis management team must consider when responding to cross-border discovery demands: legal obstacles to foreign document discovery (such as data protection and blocking statutes), cultural differences, and privilege.

A. Legal Obstacles to Foreign Document Discovery

I. Data Protection Laws

Many foreign countries, most notably the Member States of the European Union (“EU”), have data protection laws that limit the ability of companies to gather documents and transfer them to the United States for production in an investigation or lawsuit. In particular, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the “Data Protection Directive”) provides the framework for data protection in the European Union.\(^{48}\) This directive will be phased out by May 2018 when a new regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) takes full effect. This new regulation is discussed in detail below. Each of the EU Member States has national legislation implementing the Data Protection Directive.
Directive, and numerous other jurisdictions worldwide, including Argentina, Canada, and the members of the European Free Trade Association, have data protection laws modeled on the Data Protection Directive. Generally, these laws regulate “processing” “personal data” located in any system (including document-management systems, filing cabinets and email accounts) where the data can be accessed according to specific criteria. They also prohibit “transferring” such “personal data” to countries that do not ensure an “adequate level of protection” for the data unless certain conditions have been satisfied.49 In recent years, an increasing number of foreign jurisdictions have moved to add or strengthen data privacy regulations. Accordingly, best practices dictate that the crisis management team should move quickly to identify foreign jurisdictions where necessary data resides and to engage counsel experienced in that jurisdiction to provide up-to-date advice on the data privacy restrictions in place.

For purposes of these laws:

- “Personal data” means data tending to identify a natural person (e.g., a name, an official position, an office telephone number, a salary, or an account number).50
- Data “processing” means any operation performed on the data, including filtering or sorting it.51
- Data “transferring” means moving the data from one jurisdiction to another, including producing it in a U.S. proceeding.52

Because virtually all documents contain some amount of “personal data,” as a practical matter, the Data Protection Directive and its Member State analogues restrict a company’s ability to gather and produce documents from European locations. Many jurisdictions also include additional restrictions for more sensitive forms of personal data (e.g., health, race or ethnicity, sexual orientation).53

Document production from a Member State to the United States is particularly difficult because the European Commission has not found that the United States provides an “adequate level of protection” over personal data given the relative ease with which third parties can obtain documents produced in a proceeding through public access to court records, state sunshine laws, and the Freedom of Information Act.54 In addition, other than targeted legislation for health and financial records, the United States does not have a comprehensive law requiring private entities to protect personal data under their control.

In October 2015, the Court of Justice of the European Union struck down the Safe Harbor agreement that permitted the free flow of information between the United States and the European Union (provided that certain conditions were met).55 Since then, the United States and the European Union have been negotiating a “Privacy Shield” agreement. In February 2016, the European Commission issued the legal texts of the proposed “EU-U.S. Privacy Shield.” According to a contemporaneous press release, “[t]he new arrangement will provide stronger obligations on companies in the United States to protect the personal data of Europeans.”56 Specifically, the new agreement includes “strong obligations on companies and robust enforcement,” “clear safeguards and transparency obligations on U.S. government access,” “effective protection of EU citizens’ rights with several redress possibilities,” and an “annual joint review mechanism.”57 The privacy shield will work by allowing “American companies [to] register to be on the Privacy Shield List and self-certify that they meet the requirements.”58 The certification must be completed on an annual
On July 12, 2016, the European Commission formally adopted the EU-U.S. Privacy Shield, which now serves as a privacy self-certification framework that will enable companies to transfer personal data from the European Union and the three European Economic Area member states to the United States—in the EU’s view, the United States does not have “adequate” data protection laws in place. In the United States, the Department of Commerce will monitor compliance with the Privacy Shield, which is subject to enforcement by the Federal Trade Commission. Recourse for noncompliance may involve sanctions or loss of eligibility to use the Privacy Shield.

Although the Data Protection Directive generally permits the transfer of personal data that is necessary on important public-interest grounds, or for the establishment or defense of legal claims, the availability of these exemptions depends upon the nature of the proceeding and the restrictiveness of the Member State’s data protection legislation.

In 2012, the European Commission produced a draft of the General Data Protection Regulation (“GDPR”), the final text of which was agreed in December 2015. The GDPR imposes new obligations on businesses and, importantly, affects any company in the world that processes personal data of EU residents, even if the company does not have an office there. The GDPR went into effect on May 24, 2016, and will apply beginning May 25, 2018. This new regulation heightens protection for personal data and calls for stronger enforcement of data protection rules. It also substantially increases penalties, permitting fines of up to 4% of global annual turnover for non-compliant companies. Specifically, the GDPR imposes significant obligations on companies related to data breaches that create a significant risk. Among other requirements, the GDPR directs companies to provide notice within 72 hours of discovering the breach and holds data controllers and data processors jointly liable for data breaches.

The new regulation also is intended to make international cooperation easier by: (1) providing “clear rules on when EU law applies to data controllers outside the EU, in particular, by specifying that whenever controller’s activities are related to the offering of goods or services to EU individuals, or to the monitoring of their behavior, EU rules will apply”; (2) “streamlin[ing] adequacy decisions that allow free flow of information between the EU and non-member countries;” and (3) “making legitimate transfers easier and less burdensome by reinforcing and simplifying other rules on international transfers.” Although the GDPR will automatically become part of the law of EU Member States, each has some flexibility as to how many elements of the new regulation will apply within that Member State. Accordingly, as the new regulation is implemented over the next two years, there will be significant changes in the legal landscape for data protection throughout the European Union. Where EU-based data is involved, the crisis management team should engage with expert counsel to assess the restrictions then in place, as well as any coming additions to the regulatory framework.

The complexity and reach of the data protection regulations in place in the EU underscore the importance of obtaining local expertise and incorporating this expertise into an overall crisis management strategy as early as possible. In February 2009, the Article 29 Working Party, which is a body comprising representatives from the Member State data protection authorities and other officials, and which provides guidance to the Member States on data protection, issued a working document confirming that preserving documents in private civil litigation in response to a “freeze memo” constitutes “processing” under the Data
Protection Directive. Accordingly, assessing a company’s data protection exposure and formulating a solution to address it must be done immediately—in conjunction with assessing the company’s normal records-retention practices in the first hours of a crisis. For example, it may be prudent to ensure that data is not transferred to unprotected jurisdictions during the freeze process. In addition, corporate data policies should inform employees, in advance, that preservation may be required in the event of threatened or pending proceedings.

As noted above, recently many jurisdictions outside the EU also have added or augmented data protection laws. For example, in China, no comprehensive data protection law exists; however, a patchwork of data protection decisions and laws impose obligations on data controllers operating in China. Generally, companies that collect and use personal information are required to: (1) “comply with the principles of legitimacy, rightfulness and necessity when collecting and using personal information,” (2) “specify and comply with their policies regarding the purpose, manner and scope of collecting and using personal information,” and (3) “obtain consent from any individual that has information collected.” In 2015, China clarified its definition of “personal information of users” to include information that can be used to identify the user when used independently or when combined with other information, and information that concerns the time and locations of the users’ use of service that is collected by telecom business operators internet service providers during their provisions of services.” There are no generally applicable rules for transfer out of China; however, “the processing of personal information collected by commercial banks, must be stored, handled and analysed within the territory of China and such personal information is not allowed to be transferred overseas.” As discussed below, China also imposes restrictions on the transfer of “state secrets,” a category of information with an imprecise definition under Chinese law.

Companies also should be aware of the ongoing legislative debate concerning China as a cybersecurity threat. The U.S.-China Economic and Security Review Commission, which was established to “review the national security implications of trade and economic ties between the United States and the People’s Republic of China,” released a report in March 2012 assessing the network security threat from China. In light of the report – although there is still an absence of broader cybersecurity legislation – energy and defense businesses, businesses in regulated industries, and those that have a large number of government contracts may want to carefully review and update cybersecurity policies prior to signing significant new contracts with foreign providers of telecommunications equipment and services, or with those who source their equipment overseas. Investment from China and major contracts with Chinese providers will continue to receive particular scrutiny from government bodies.

2. Blocking Statutes

Blocking statutes are another impediment to cross-border discovery. These statutes generally prohibit data transfers from one country to another, absent specific circumstances. For example, French Penal Code Law No. 80-538 prohibits persons from seeking or disclosing any documents in a foreign proceeding unless otherwise authorized, for example, by the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. This statute, which carries criminal sanctions, applies to any person within French jurisdiction who violates it, including a Paris-based subsidiary of a
Crisis Management: in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in a Global Environment

Copyright © 2016 Association of Corporate Counsel

A multinational corporation that produces documents from France in a lawsuit in the United States.

China’s Law of the People’s Republic of China on Guarding State Secrets can be considered a blocking statute as a practical matter. It criminalizes transferring “state secrets” out of China. State secrets include information relating to national security and other interests whose transfer could harm security in the fields of politics, economics, national defense, and diplomacy, among others. From the perspective of a U.S. practitioner, the limits of the law are unclear. Again, the crisis management team should incorporate local experts to assess and help mitigate a company’s exposure under the state secrets law.

Japan implemented a new state secrets law in December 2014. The new law “provides for the protection of information in the categories of defense, diplomacy, counter-terrorism and counter-espionage.” The previous law limited the punishment for Japanese citizens to one year, excluding defense officials who could be imprisoned for five to ten years. The new law provides that government officials and defense industry employees can face up to ten years in prison and a 10 million yen fine. Also under the new law, journalists and activists who solicit information that is deemed to be a state secret can be imprisoned for up to five years for conspiracy to solicit state secrets, and up to ten years if they actually acquire the information. The mechanism for determining what constitutes a state secret under the new law is “entirely in the government’s hands.” In its first year in force, 382 state secrets were designated under the new law.

3. Foreign Data Privacy Restrictions and U.S. Courts and Regulators

United States regulators and courts generally are not sympathetic to companies’ claims that they are prevented from producing documents by foreign data protection laws or blocking statutes. For example, in investigations by the U.S. Department of Justice (DOJ) or the Securities and Exchange Commission of possible securities law violations involving documents located in Europe, the agencies usually take the view that their investigations are within the “public interest,” and that companies therefore must comply with their document requests under that exemption to Data Protection Directive, even if the relevant Member State’s data protection regulator may not agree. On April 5, 2016, the Fraud Section of the Criminal Division of the Department of Justice released its Enforcement Plan and Guidance regarding the Foreign Corrupt Practices Act (“Enforcement Plan”). The Enforcement Plan outlines a “pilot program” for “motivating companies to voluntarily self-disclose FCPA-related misconduct.” In order to receive credit for full cooperation under the pilot program, companies will be expected to disclose “overseas documents, the location in which such documents were found, and who found the documents.” Exceptions will be allowed where foreign data privacy law prohibits disclosure, but “the burden is on the company to establish the prohibition.”

The liberal discovery rules in U.S. courts can make it difficult to balance production obligations and foreign data privacy restrictions. In Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, the United States Supreme Court held that two French government-owned corporations were required to respond to discovery requests propounded under the Federal Rules of Civil Procedure, and not the Hague Convention, even though producing documents under such circumstances would violate the French blocking statute. U.S. courts have been split on whether the possibility of
criminal penalties in the home country of a party opposing a discovery request on blocking-statute grounds is an element they will consider in ruling on a motion to compel discovery.\textsuperscript{82}

Given the tension between foreign data protection and blocking statutes and the United States’ strong public policy in favor of open and broad disclosure, whether in the context of litigation or regulatory action, a crisis management team must be very cautious in its approach to cross-border productions. The company must address each jurisdiction’s requirements with an ultimate view toward a global resolution of the proceeding. The company also should be prepared to present and defend with specificity any data privacy restriction that it feels prevents disclosure.

**B. Cultural Differences**

U.S.-style litigation and internal investigations largely are alien to foreign organizations. Accordingly, if a company plans to gather data from its foreign offices, it also must take into account local customary practices regarding information privacy and ownership. For example, most U.S. employees are accustomed to the idea that their work computer and email accounts belong to their employer. Outside the United States, however, the understanding frequently is the opposite: an employee’s computer and email account are private, and it may be a criminal offense for the company or its attorneys to invade that privacy. Indeed, employee-data collection outside the United States may be seen as coercion by an employer, and it may lead to labor-union grievances or complaints. The company’s crisis management team must understand these cultural differences, which often are expressed in foreign employment and labor relations law, in formulating a strategy to gather documents from the company’s employees for production in any proceeding.

**C. Privilege**

Section X of this InfoPAK\textsuperscript{SM} discusses waiving privilege in parallel proceedings, and the risks and possible strategic advantages of doing so. Whether to waive privilege—and, more fundamentally, whether to assert privilege—is more complicated when proceedings involve documents from jurisdictions outside the United States. This is because the substantive law of privilege varies across jurisdictions, particularly in Europe. In September 2007, the European Court of First Instance issued its opinion in *Akzo Nobel Chemicals Ltd. v Commission of the European Community*,\textsuperscript{83} reaffirming that in EU litigation, communications between a company’s employees and in-house counsel are not privileged. The *Akzo Nobel* rule applies when EU agencies are involved in an investigation or litigation. When a Member State agency leads the investigation, however, the Member State’s substantive privilege law, which may differ from the EU rule, applies. In the United States, of course, such communications are privileged.\textsuperscript{84}

Accordingly, in a parallel proceeding in the United States, whether the company can claim privilege over a document generated in Europe may turn on whose privilege law applies to it. Generally, United States courts apply United States privilege law when a document reflects a communication that “touches base” with a United States legal interest.\textsuperscript{85} Some United States courts apply a balancing test in determining whose privilege law applies,
upholding the law of the jurisdiction with the strongest interest in the subject of the communication, unless the foreign law offends United States public policy. Accordingly, in determining when to withhold documents from production, the company’s crisis management team must assess the entire legal framework for doing so.

The same is true when deciding to produce protected documents. When a parallel proceeding involves an investigation by a foreign regulator or prosecutor, particularly in Europe, a company must assess how the global privilege framework will multiply the ramifications of the decision. In the United States, waiving privilege as to one document generally results in a waiver of the privilege as to all documents concerning the same subject matter. The company therefore must consider the possibility of follow-on litigation or enforcement in the United States if it elects to produce a privileged document to a European regulator as part of a cooperative effort there, even though subject-matter waiver generally is not established in Europe. Again, the crisis management team must take a global view in addressing every constituency; the fact of multiple proceedings in multiple jurisdictions means the company may have to make different choices than it would if faced with a single investigation or lawsuit in a single jurisdiction.
VI. Interacting with Insurers and Auditors

In addition to interacting with the media and perhaps foreign jurisdictions in connection with cross-border discovery, companies faced with a crisis also should be prepared to interact with numerous other third parties, including their own insurers and their outside auditors.

A. Insurance Coverage

A corporate crisis inevitably will raise insurance coverage issues, and coverage issues are likely more complicated with the increased complexity of a crisis. Advance preparation and careful steps early in the crisis are essential to navigating these difficult issues.

Insurance is purchased to transfer or manage risk of extraordinary events. Accordingly, it is crucial to understand the range and scope of insurance coverage and fill any gaps that are identified in such analysis. A single event or related series of events are likely to raise coverage issues under several different insurance policies, including directors and officers (“D&O”) policies. Advance familiarity with the policies, including an ability to quickly identify them, is important to managing the early stages of a problem. Delay, or failure to identify relevant policies, may compromise a company’s coverage, making it harder and more expensive to resolve the crisis in its later stages.

Traditional insurance policies might cover cyber losses, but there has been a continuing trend toward broad cyber exclusions in insurance policies. However, more insurers are offering, and more companies are procuring, specialty cyber policies. Indeed, in its October 13, 2011 guidance for public companies regarding disclosure obligations for cybersecurity risks and cyber incidents, the SEC stated that “[a]ppropriate disclosures may include a description of relevant insurance coverage.” The purchase of cyber insurance is on the rise – with financial institutions comprising the largest percentage of companies buying the specialty insurance. In-house counsel and other relevant personnel should evaluate the organization’s cyber risk profile to determine the appropriate cyber insurance to purchase. This assessment consists of evaluating, among other issues, how personal data is stored, how access to IT systems is controlled, and the jurisdictions in which the company operates. Obtaining specialty cyber insurance is one part of developing a comprehensive strategy to mitigate and manage cyber risks.

Equally important is appropriately tempering the content of early notifications to insurers. When a crisis hits, but relevant facts and parties have not yet been identified, a company likely will not have decided on its comprehensive strategy or its position on specific issues that have arisen. In communicating with insurers, a company should provide adequate notice as required under the policy, but also should be careful not to stake out a position that could conflict with managing other aspects of a problem.

Once notice has been provided, there likely will be little or no benefit to engaging in a coverage dispute as a crisis unfolds. It may be far more prudent to defer any substantive interactions or disagreements to a point where additional facts have been gathered and the company’s comprehensive strategy has been developed. When coverage issues are
postponed to the conclusion of the matter, a company should keep in mind that documents and communications with counsel related to the matter likely will be relevant to insurance coverage disputes. Indeed, a company may elect to waive privilege regarding communications with counsel in the underlying case when those communications support the company’s position in a follow-on coverage dispute. Accordingly, counsel in the underlying matter should be apprised generally of the coverage issues and directed to maintain documents as they are created.

Furthermore, counsel should consider and prepare for the possibility that insurance carriers will deny coverage. Thus, it is often best for counsel to identify experienced insurance counsel early in the matter to assist the company in navigating the notice requirements and then to be available to challenge any inappropriate coverage decisions.

B. Independent Auditors

For a public company, interactions with its independent auditor are a key aspect of managing any crisis. In some scenarios—for example, if information revealed during a quarterly review or annual audit triggers an auditor’s obligation to seek an investigation of potentially illegal activity—the auditor may be the first to raise an issue. When a crisis arises in other contexts—such as a lawsuit, government investigation, or whistleblower allegation—the auditor likely will be among the first constituencies demanding real-time fact gathering and access to information. Recent enforcement actions and litigation against accounting firms have heightened their sensitivity to risk and have prompted auditors to closely monitor any situation that can affect a public company’s financial picture. Companies also should consider external audits of privacy and cybersecurity policies and processes, as an audit will not only minimize the risk of a cyber incident, but also provide regulators with comfort. Company counsel can better coordinate with the company’s auditors in such situations by understanding auditors’ statutory responsibilities and continuously assessing any situation as it unfolds.

This section briefly outlines the legal framework through which auditors analyze potentially improper conduct at a public company, with a focus on Section 10A of the U.S. Securities Exchange Act of 1934, 15 U.S.C. § 78j-1 (“Section 10A”). Next, it discusses potential responses to an auditor’s demands for information about a crisis or potential illegal act. Finally, it addresses the attorney-client privilege and attorney work product protection in communications with an independent auditor during a crisis.

I. Understanding the Section 10A Framework

Under U.S. federal securities laws, an independent auditor has specific statutory obligations if it learns of potentially illegal conduct through an audit. Specifically:

- During the course of any audit, if an auditor becomes aware of information indicating that an illegal act has or may have occurred, the auditor is required to determine whether it is “likely” that an illegal act has in fact occurred.
- If the auditor determines that it is “likely” that an illegal act occurred, the auditor must (i) determine the possible effect of the illegal act on the company’s financial statements and (ii) inform the appropriate level of management and ensure that
the audit committee of the board of directors (or the full board in the absence of an audit committee) is adequately informed, as soon as practicable, unless the illegal act is “clearly inconsequential.”

- If an illegal act has been detected, the auditor is required to report, as soon as practicable, its conclusions directly to the company’s board of directors if it concludes that: (i) the illegal act will have a material effect on the company’s financial statements; (ii) the company has not taken “timely and appropriate remedial actions”; and (iii) the failure to take remedial actions is reasonably expected to warrant departure from a standard report of the auditor, or warrant resignation from the audit engagement.

- A Section 10A report from an auditor triggers certain reporting obligations by the board of directors. In particular, the board of directors has one business day to inform the SEC that it has received the report and give the auditor notice that it so informed the SEC. An auditor that does not receive such notice must either resign from the engagement or furnish the SEC with a copy of its report.

In assessing how an auditor is likely to respond in a Section 10A situation, counsel should take into account that the trigger for potential investigation under Section 10A is low. First, the statute creates obligations for an auditor when the auditor learns of information indicating that an illegal act “has or may have occurred.” Thus, the auditor’s duties come into play upon discovery of the possibility of an illegal act, not just a finding that such an act occurred. Second, the statute specifies that even an immaterial potential illegal act must be investigated. An auditor’s responsibility to inform senior management and the audit committee of an illegal act is not based on the familiar “materiality” standard, but rather a “clearly inconsequential” standard. Third, what constitutes an “illegal act” is broadly defined in Section 10A to mean “an act or omission that violates any law, or any rule or regulation having the force of law.”

2. Responding to an Auditor’s Section 10A Notification

Once an auditor identifies the possibility of an illegal act—either as a result of other events in a corporate crisis, or as the first indication of the potential issue—the auditor usually will expect a company to investigate fully whether an illegal act in fact has occurred. This is because, based on Statement on Auditing Standard 54, independent public accountants generally take the position that determining whether an act is illegal is outside of their professional scope and must be based “on the advice of an informed expert qualified to practice law.” In a traditional Section 10A situation, a company generally commissions an investigation of the potential act, either by internal resources or outside counsel, and sometimes with oversight of the company’s audit committee. In a crisis situation involving many potential constituencies, additional factors come into play in managing the investigation:

- Give careful consideration to who will conduct the investigation, who will oversee it and its scope. Where there are several constituencies and potential sources of liability, or where the auditor has raised questions about management’s integrity or representations made to the auditor, the company may be more comfortable with, and the auditor may expect, an audit committee or special litigation committee overseeing an investigation by external counsel.
Communication between the issuer and auditor on the scope and the nature of the investigation—soon after an issue arises—may assist in addressing concerns an auditor may have when a crisis occurs. Counsel overseeing the response to the crisis should consider early and frequent communications with the auditor regarding the process that will be used to investigate facts, who will oversee the process and the topics it will cover.

■ Careful consideration should be given to the manner in which interim and final fact-finding results are reported to the auditor. At the very least, the auditor will seek, during its review and audit processes, representations about the potential impact of the events underlying the crisis. In addition, even if not in a formal review period, an auditor frequently will seek real-time updates on a company’s investigation of and response to a crisis. Counsel overseeing the response to a crisis should carefully consider the manner in which such updates are provided. Auditors may prefer written summaries and information; however, until an investigation is completed, these may not always be available. In addition, as discussed more fully in Section VI.B.4, the government and private litigants may take the position that disclosure of otherwise privileged materials to an independent auditor waives the privilege. Thus, oral updates may be most prudent as a crisis unfolds. Counsel should be aware, however, that even when a company provides oral briefings to its auditors, the auditors will usually take notes and include written summaries in their work papers.

■ A company should consider appropriate real-time remedial measures. Section 10A contemplates that, if the investigation identifies an illegal act that has a material effect on the company’s financial statements, management will take “timely and appropriate” remedial action. Such action could include personnel actions, restatement or other adjustments to prior financials, adjustments and disclosures in current financial statements, changes in accounting policies or treatments and changes in internal structure, processes, and procedures. As a practical matter, keeping the auditor apprised of the investigation’s status and the company’s contemplated actions will greatly reduce the possibility that the auditor will deem the company’s remedial actions unacceptable.

3. Preparing for the Worst-Case Scenario

The fluid and evolving nature of a corporate crisis poses particular problems in the context of a quarterly review or annual audit. Depending on the nature of issues or acts that have arisen, the auditor may not be comfortable continuing to perform work in connection with a quarterly review or an annual audit.

In particular, if the auditor believes that the conduct identified raises questions about the integrity of management from which information and representations are required, the auditor may conclude that all work, or work on certain aspects of the review or audit, must be suspended until completion of the investigation. This “pencils down” approach is likely to delay an issuer in obtaining auditor approval of its quarterly and/or annual financial statements.

Alternatively, the auditor may be willing to continue review or audit work, but be unable or unwilling to complete the review or conclude the audit until the investigation is finished.
Either scenario may delay the filing of the financial statements, which raises public disclosure issues and other questions for the company.

Finally, even where a company is doing all it can to manage an auditor’s expectations, an independent auditor may be reluctant to provide an unqualified audit opinion in the midst of a corporate crisis. A qualified audit opinion, either at a quarterly review or annual audit, could have far reaching consequences that deepen the crisis, as it may result in, for example, breaches of lending or financing covenants.

A company should prepare for the full spectrum of auditor responses to parallel proceedings and corporate crises.

- At one end of the spectrum, the company should consider whether it can assuage concerns of the auditor and secure timely filing of periodic reports with the SEC. In such a situation, careful consideration should be given to whether an internal or independent effort can provide sufficient resources to allow for a timely completion of a thorough investigation that will facilitate the issuance of the auditor’s opinion.

- At the other end of the spectrum, the company should anticipate that an auditor may decide to withdraw from the audit. Careful consideration should be given to whether the company wants to work to convince the auditor not to withdraw. Because the company often lacks leverage with its auditor during a corporate crisis, the company should take preliminary steps to be in a position to promptly replace the withdrawn auditor with a new auditor.

- During the crisis, the auditor’s concerns may result in delayed filings or qualified opinions. Careful consideration should be given to the different collateral consequences attendant to the potential outcomes along the spectrum and the effort needed to move an auditor from a less favorable outcome to a more favorable outcome.

Planning for the foregoing scenarios should recognize, however, that a company may have very little leverage with respect to withdrawal, selection of a new auditor or an auditor’s decision to delay its opinion or issue a qualified opinion.

4. **Addressing Special Concerns Regarding Sensitive Information Provided to Independent Auditors**

Since the corporate accounting scandals of 2001 and 2002, and the passage of the U.S. Sarbanes-Oxley Act of 2002, auditors have placed increasing demands on the companies they audit for information relating to Section 10A or company-initiated investigations that may otherwise be covered by the attorney-client privilege or the attorney work product protection. Auditors once largely limited the legal information requested to audit letters given pursuant to the American Bar Association’s Statement of Policy Regarding Lawyers’ Responses to Auditors’ Request for Information and the American Institute of Certified Public Accountants’ Statement of Auditing Standards No. 12. More recently, auditors have sought evaluations of litigation reserves, legal opinions on tax and other matters and reports on the outcome of internal or independent investigations that often accompany parallel proceedings. Indeed, an auditor may insist that a Section 10A investigation cannot
be completed, audit work started or completed or an opinion issued, without access to this information.

Company counsel should carefully consider that sharing information with auditors may lead a litigant to assert, or a court to conclude, that there has been a waiver of the attorney-client privilege or the attorney work product protection. Companies should make decisions about when to share information and what information to share after consideration of potential waiver issues.

Several courts in the United States have held that disclosure of attorney-client communications to an independent auditor will waive the privilege with respect to those communications. Some states have developed common law supporting, or have codified, client-accountant and client-auditor privileges that may extend the umbrella of confidentiality over attorney-client communications that are disclosed to independent auditors. The state privileges, though, may be limited to matters before the state courts within those states that have such privileges. Federal common law generally does not recognize such an extension of the attorney-client privilege. And at least one state court rejected a state law privilege claim based on the accountant-client privilege law of the state where the client and auditor were located.

The law on disclosure of attorney work product is even less clear as federal courts have reached differing conclusions as to whether, in the ordinary course, an independent auditor is sufficiently adverse to defeat the work product protection.

Given the potential for waiver of the attorney-client privilege and work product protection as a result of disclosures to an independent auditor, company counsel must be prepared to confront the waiver issues associated with regular and extraordinary communications with auditors. As a prophylactic measure, auditor engagement letters should contain confidentiality provisions. The existence of such a provision may provide some support against a waiver argument. As a reactive measure, company counsel should regularly evaluate whether to share the results of an internal or independent investigation with the company’s auditor. Company counsel should consider factors such as the likely harm from waiver versus the benefits of disclosure to the auditor, the likelihood that an enforcement authority will seek “voluntary” disclosure of the investigation results, and the other potential advantages to disclosing the investigation report.

Finally, the company may be able to structure the manner in which information is shared to maximize arguments against waiver. If the company is attempting to preserve the privilege and protection, it may be helpful to limit the briefing to the underlying facts and not include any of the analysis or impressions of counsel. Because monitoring and analyzing information provided to the auditor in connection with a Section 10A investigation is an element of the auditor’s procedures, auditors usually document the information that has been provided to them in their work papers. Thus, even where information has been shared orally, auditors likely will have a written summary of investigation issues that may be sought by regulators or in civil litigation.
VII. Communicating with the Government

In many instances, a corporate crisis also will lead to contacts with government enforcement authorities and regulators. Government interest can be driven by media reports, customer complaints, consumer groups, confidential informants, industry regulator updates, government inquiries, or the company’s own voluntary self-reporting. In any of these scenarios, government contact can present formidable challenges as companies balance their obligations to the government, the company, and the public. In advance of a crisis, however, companies can take steps to prepare by understanding the key issues and strategic concerns likely to arise.

Before any crisis, a company should be aware of the broad array of government authorities that may be interested in both the company and its individual employees. In some cases, investigations can involve a cascade of independent but parallel inquiries by the U.S. federal government, state-level authorities, and foreign authorities. These competing inquiries potentially invite both tension and opportunities for cooperation as a company assesses its options. Both U.S. and foreign authorities, for example, increasingly are coordinating their investigations, including the sharing of information and evidence. Companies may be asked to facilitate this coordination by agreeing to waivers permitting authorities to share otherwise statutorily confidential information. Agreeing to do so, of course, will require a company’s attention to issues including the staging of information to different regulators, consistency of the material provided, and the timing of any potential resolutions that may result.

This section explores how to navigate governmental authorities tasked with regulating and investigating a company’s conduct, including cooperating with and reporting to government authorities. Companies facing a corporate crisis that might involve interactions with government authorities should consider retaining experienced outside counsel to help guide the company through the process of cooperating with, and reporting to, government regulators and enforcement agencies.

A. Knowing the Company’s Regulators and Enforcement Authorities

A company should be aware of and maintain a list of the key government contacts with which it interacts. Whether domestic or foreign regulators, the company will benefit from establishing an open and forthcoming relationship in advance of a crisis, and appropriately updating the company’s regulatory supervisors. Laying the groundwork for these relationships with this kind of regular outreach bolsters a company’s credibility in the event of a crisis, and in any potential response to related government inquiries.

- **U.S. Federal Regulators.** In addition to investigative agencies such as the Department of Justice and Securities and Exchange Commission, a company should expect to interact with its specific federal regulators in any crisis. These agencies are a key constituency and in many cases will be recognized by a company as its highest priority government contacts. These regulators have significant power in the highly regulated environments in which many
companies operate, including financial services, health care, manufacturing, government contracting, the environment, or some combination of the foregoing.

- The crisis management team should be aware of the key contacts internally and at each regulator. Recent interactions with relevant regulators also should be noted, including, and especially, any contentious issues that have arisen or are currently pending.

- The regulatory climate, industry trends, and recent interactions between a company and its regulator will affect a company’s strategy during a crisis. This information should be gathered as early as possible when an issue surfaces.

**U.S. State Regulators.** In addition to federal authorities, a corporate crisis frequently will be spurred by, or attract the interest of, state regulators and Attorneys General. State statutes may impose conflicting obligations or standards on a company, and states—as well as state and federal authorities—may compete to bring their respective enforcement actions. The degree of confidentiality afforded the documents and information disclosed to state regulators varies by jurisdiction and in some cases is at the discretion of the regulators.

- The crisis management team should be aware of key state regulatory and legislative constituencies in locations important to the company, such as company headquarters, locations of large manufacturing or other facilities, and significant sales bases. Contacts at the legislative, regulatory, and prosecutorial offices in each of these states should be identified.

- As an issue unfolds, the crisis management team should carefully consider coordinated responses to state regulatory inquiries. Weight should be given to states likely to most aggressively pursue or prosecute a company, as well as states that may be sympathetic allies given a company’s large presence or employment base in a particular location.

**Foreign Authorities.** It is increasingly common for U.S. federal and state inquiries to generate attention from global authorities. As between federal and state efforts, foreign inquiries also may create tension for a company in contending with international standards that at times may contradict both domestic protections and obligations. As with U.S. federal regulators, foreign authorities may exercise great influence over particular business areas and expect different standards of information sharing, including initially requesting disclosure of information a company otherwise deems privileged or confidential.

- Geographic and cultural factors are important to consider prior to responding to foreign government inquiries and can play a crucial role in the tenor and effectiveness of exchanges with international regulators. The crisis management team or the appropriate internal company contact should be aware of the key regulatory personnel, as well as recent interactions with the regulator.
• As noted, in light of increased communication and coordination among international authorities, a company should expect that information provided to one regulator may be shared with others.

■ U.S. Congressional Inquiries. Depending on the nature of the crisis, it is possible that the company may receive inquiries from Congress, including requests for information and public testimony by company representatives. In response to public demands, Congress may move quickly in seeking such testimony, which may result in key witnesses publicly testifying while a company is in the midst of its ongoing investigation.

• Based on company locations, history, constituencies, and similar factors, the crisis management team should assess which legislators are likely to be aggressive in their criticisms and investigation of the company, and which legislators are likely to be sympathetic.

• The crisis management team should carefully assess the costs and benefits of voluntarily providing information in response to congressional inquiries. A failure to fully share information may create short- or long-term antagonism, reputational harm, and negative publicity. However, information provided to Congress may be public or become public, and members of Congress may publicly use inflammatory information for political purposes ultimately harmful to the company.

Any combination of government inquiries—U.S. federal, state, foreign, and congressional—requires management of shifting and competing priorities. Depending on the volume of government contacts received and the nature of the government authorities, a company should consider whether to engage outside counsel to coordinate both interactions with the government and the resulting internal work at the company. For inquiries involving cross-border investigations or international regulators, a company may select various local or regional counsel to manage different geographically-based inquiries (e.g., North America, Europe, Asia-Pacific), opt for global coordinating counsel to oversee all regions, or employ a combination of both. What will work best for a company will depend on the nature of the crisis, the volume of government contacts, and the jurisdictions at issue.

B. Cooperating with Government Entities

A company gathering facts in response to a crisis will be faced, typically early on, with the question of whether to voluntarily disclose that information to one or more government authorities.

Providing information to the government may be necessary to preserve a relationship, demonstrate cooperation, or minimize liability in the forms of charging, sentencing, and financial penalties. A company’s industry regulators may request (or demand) information in connection with ongoing regulatory oversight or in connection with a required approval, permit, or license. Securities regulators and law enforcement agencies also may seek information in an investigation, with the DOJ and SEC among those providing incentives for a company to fully cooperate with government investigators. In assessing disclosure and cooperation with the government, a company also should consider the government’s
growing priority for holding culpable individuals accountable in government investigations.

- **Cooperation with the U.S. Department of Justice.** When determining whether to charge a company with a criminal violation or to resolve a corporate criminal case by means other than indictment, the DOJ analyzes factors outlined in Section 9-28.000 of the U.S. Attorney’s Manual (“USAM”), which has been reinforced by recent DOJ guidance. These factors include a corporation’s timely and voluntary disclosure of wrongdoing, thoroughness and speed in investigating, the proactive nature of its cooperation, a company’s existing compliance program, and remediation efforts. The DOJ’s recent emphasis on rigorous compliance programs is exemplified by the DOJ’s newly created Compliance Counsel Expert position. In this role, the Compliance Counsel is dedicated to assessing companies’ claims about their compliance efforts, including consideration of program designs, operations, communications, and resources.

Even prior to consideration of these factors, however, a company’s eligibility for any “cooperation credit” turns on the disclosure of all facts about individual culpability to the DOJ. Memorialized in a 2015 memorandum by Deputy Attorney General Sally Quillian Yates (“Yates Memorandum”) and related USAM revisions, new DOJ guidance builds on the previously established cooperation factors and provides:

- Any cooperation credit now relies on a corporation disclosing to the DOJ all facts relating to potential individual misconduct—including identities of potential wrongdoers—regardless of individuals’ positions or seniority.
- The criminal and civil DOJ divisions are increasingly coordinating to focus on individual culpability from the outset of an investigation.
- Departmental approval is now required for DOJ attorneys to decline to bring charges against individuals, with the Department not releasing individuals from civil or criminal liability absent extraordinary circumstances.

Notably, the USAM also specifies that “[e]ligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection,” and that federal prosecutors are prohibited from seeking waivers of privilege except in very limited circumstances. According to the USAM, cooperation will not turn on “whether the corporation discloses attorney-client or work product materials.”

If a company meets the new threshold requirements regarding individual culpability, it will be eligible for credit—the extent of which will depend on the aforementioned broad assessment of the corporation’s cooperation. This credit, however, will not be precluded if a company has been unable to identify the culpable individuals following a thorough and appropriate tailored review, as long as the corporation has provided relevant facts and otherwise assisted the DOJ with obtaining evidence in its investigation.
Cooperation with the U.S. Securities and Exchange Commission. Cooperation also plays a significant role in SEC investigations into corporations and individuals, including decisions regarding the enforcement tools available to the Commission. The SEC considers four broad factors outlined in SEC Accounting and Auditing Enforcement Release No. 1470 ("Seaboard factors") when evaluating a company’s cooperation, and in determining whether to refrain from taking enforcement action: self-policing, self-reporting, remediation, and cooperation. More specifically, the SEC will consider:

- Whether the results of the company’s review, as well as all relevant documentation, are shared with the SEC Staff;
- Whether information is disclosed to the staff that was not requested and otherwise might not have been discovered;
- Whether the information shared is thorough and reliable so that it may be used by the staff to facilitate prompt enforcement action against those who may have violated the law;
- Whether results of internal investigations are memorialized in a writing and shared with the staff in a format that can be used in an enforcement proceeding; and
- Whether the company encouraged its employees to cooperate with the staff’s investigation and whether efforts were made to secure such cooperation.

The SEC’s 2010 “Enforcement Cooperation Initiative” builds on this foundation, providing for the use of cooperation agreements, deferred prosecution agreements (“DPAs”), and non-prosecution agreements (“NPAs”), with far more cooperation agreements (80) under the Initiative than DPAs and NPAs combined (10). In addition, the SEC improved its process for submitting immunity requests to the DOJ.

Consistent with the DOJ Yates Memorandum, the SEC also is promoting an increased focus on individuals implicated in corporate misconduct, with the Commission emphasizing the need for a company to share information about individuals to receive cooperation credit, including facts involving senior officials. Moreover, for individuals themselves, the SEC also has articulated factors in evaluating the significance of cooperation by those individuals.

As reflected in the DOJ and SEC’s recent shifts in focus, government authorities are facing growing pressure and mounting criticism related to prosecutions of corporate individuals. For a company and its officers, directors, and employees, the link between full cooperation and individual culpability increases the potential for conflicts between the company and individuals. As a result, companies will need to consider whether to provide counsel for individuals at the outset of government contact and throughout the process as new facts and information are learned. Even where no issue is found at the beginning of an investigation, the interests of a company and its employees ultimately may not align, particularly in situations where facts related to individual misconduct are uncovered. In the event individuals are represented by independent counsel, this also may affect a company’s ability to fully cooperate with government requests related to those individuals.
Crisis Management: in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in a Global Environment

C. Reporting to Government Entities

Whenever a company concludes that its crisis management strategy will include reports to government authorities about the company’s fact-finding, careful consideration should be given to the manner, scope, and timing of that reporting.

- **Clear and Complete Reports.** Government regulators expect clear and complete reporting and usually ask a company to provide a distillation and analysis of key factual findings and remedial measures. Such presentations are most effective after an adequate internal inquiry has been completed to assure that the available facts are known. Accordingly, where possible, a company should structure its reporting to follow its investigative plan. In some cases, however, the government may demand interim or real-time updates. In such instances, a company should be careful to frame interim reports with the knowledge that its understanding of the facts may—and often does—change. Where the government has raised specific questions regarding the facts and circumstances of the company’s actions, a persuasive presentation will require the company to address those points directly.

- **Balanced Reports.** Presentations are frequently most effective if a company presents a balanced view of the conduct, including both those factors that support and those that disfavor the company. To accomplish this objective, a company should anticipate that it is providing the government with a blueprint of its defense of a potential case. This may include furnishing exculpatory documents of which the government is as yet unaware, as well as proffers of testimony that the company expects to be available from particular witnesses. In so doing, the company may well be sacrificing any advantage of surprise that it might otherwise obtain if the case ultimately were to proceed to indictment and trial or other enforcement proceedings. By submitting such information, a company may enable the government to anticipate and counter its defenses to the possible charges of misconduct. In a situation involving multiple issues and parties, such disclosures to the government also may be sought by private litigants, giving them an understanding of the company’s defenses. Thus, a company’s strategy for reporting to the government should weigh the advantages and disadvantages of full disclosure.

- **Oral Versus Written Reports.** A company also should carefully consider whether to report orally or in writing to the government. Written reports may be preferred by the government, and foreign authorities may insist on written submissions in light of jurisdictional traditions and customs, or more practical concerns with potential translation issues. However, a company’s understanding of information early in an investigation may change as further facts are developed, and written reports cannot be undone—only corrected or updated. In addition, a company generally should be mindful that sharing a written report with one government agency may lead to disclosure to other agencies and parties, both domestically and abroad. For example, U.S. federal law enforcement agencies may be permitted or feel compelled to share reports with other agencies and may already have international information sharing protocols in place. Similarly, civil litigants have a sophisticated understanding of the kinds of materials requested by government agencies, and they are likely to
seek these same materials—including a company’s written reports or summaries—in litigation. For these reasons, in the early stages of an investigation, a company may decide to provide information orally to the government in meetings or telephone updates.

In a crisis situation, tradeoffs are inevitable. Insisting on an oral report to the government may benefit a company because it avoids creation of a potentially non-privileged, discoverable document that sets forth the company’s preliminary findings. However, the government may be less satisfied and more hostile if it does not receive written reports. In addition, in oral communications with the government, there is the potential for miscommunications or misunderstandings.
VIII. Meeting the Company’s Public Disclosure Obligations

Separate from the issue of disclosures to insurers, auditors, and government regulators, a public company managing parallel proceedings—such as an internal investigation, a governmental investigation, or civil litigation—also must consider its ongoing public disclosure obligations. A true corporate crisis invariably creates special disclosure considerations. Even if one aspect of the crisis may not lead to a disclosure obligation, the combination or interaction of events may lead to an obligation to disclose a potentially material impact of the crisis on the company’s finances or operations.

Information is material under U.S. federal securities laws if a reasonable investor would consider it important in making an investment decision. Whether aspects of a crisis—including government investigations, litigation, auditor reactions, and industry reactions—are material depends on several factors, including:

- The significance of the underlying facts;
- The company personnel involved;
- The likelihood of an enforcement action and/or litigation losses; and
- The likely impact of the crisis on the company’s revenues, profits, and similar financial metrics.

Although companies do not have a general obligation to disclose all material information, if the duty to disclose is otherwise triggered, it will be incumbent upon the company to disclose material information relating to the investigation. In addition, even if a company were to conclude that it does not have a specific legal obligation to disclose information related to the crisis, there may be pressure from various constituents to do so. Indeed, the SEC has stated in guidance that other required disclosures make necessary the disclosure of cybersecurity risks and cyber incidents.

This section discusses very generally regulatory provisions that bear on disclosure, a company’s duty to disclose in special circumstances, and situations when voluntary disclosure may be advisable. In making any disclosure decision, however, company counsel should coordinate closely with the company’s disclosure counsel.

A. Regulatory Provisions Bearing on Disclosure

No statutes or SEC rules specifically require public companies to disclose in any filing that they are under investigation. Certain provisions of the U.S. federal securities laws, however, impose obligations to disclose certain information in documents filed with the SEC. Courts have looked to these provisions for guidance in determining whether investigations should be disclosed.

SEC Regulation S-K contains the disclosure requirements for the non-financial statement portion of documents filed with the SEC.
■ **Item 103** of Regulation S-K, entitled “Legal Proceedings,” applies to required periodic filings and registration statements. This item mandates disclosure of “material pending legal proceedings” against the issuer, including a “description of the factual basis alleged to underlie the proceeding and the relief sought.” Further, Item 103 specifically requires disclosure of “similar information as to any such proceedings known to be contemplated by government authorities.” Regulation S-K does not define “proceedings.” Courts that have addressed this issue have taken the position that “proceedings” do not include an investigation and that disclosure of an investigation is not required before the government agency indicates that it is contemplating an enforcement action against the issuer.125

■ **Item 401(f)** of Regulation S-K, which applies to proxy statements, requires disclosure concerning directors or proposed directors, if such person “is a named subject of a pending criminal proceeding.” This item applies to events that have occurred within ten years prior to the filing and 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 issuer. Like Item 103, Item 401(f) does not mention investigations. Further, Item 401(f) covers “criminal proceedings” only and not “legal proceedings” generally.

■ **Item 303** of Regulation S-K, which applies to periodic filings and registration statements, requires disclosure of “any known trends or uncertainties that . . . the registrant reasonably expects will have a material . . . unfavorable impact on net sales or revenues” and any “known . . . uncertainties . . . that are reasonably likely to result in the registrant’s liquidity . . . decreasing in any material way.”

■ **Item 503(c)** of Regulation S-K, which applies to risk factor disclosures generally, instructs registrants to “not present risks that could apply to any issuer or any offering” and to “[e]xplain how the risk affects the issuer or the securities being offered.”126 In the context of cybersecurity risk disclosures, for example, this item requires that when those disclosures are made, they should be made with a great level of specificity. The SEC lists in its guidance the following potentially appropriate disclosures:

1. discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
2. to the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
3. description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
4. risks related to cyber incidents that may remain undetected for an extended period; and
5. description of relevant insurance coverage.127

While no rule or provision expressly requires disclosure of a government investigation, companies should consider whether a disclosure duty arises in the context of periodic reports that must be filed with the SEC, or where the company or a knowledgeable insider purchases or sells shares of the company.128
B. Duty to Disclose in Special Circumstances

A company also may have a duty to disclose information when new developments make the company’s prior statements materially misleading. For example, a company’s statements that its financials have been prepared in accordance with Generally Accepted Accounting Principles could be called into question if serious books and records or internal controls issues are identified in connection with an internal investigation, lawsuit, or similar fact-finding process.

Companies also should be cognizant of the requirements of Regulation FD, which addresses selective disclosure and requires that a company publicly disclose material nonpublic information made available to certain enumerated persons, including securities market professionals and holders of the company’s securities who might trade on the basis of the information provided. A corporate crisis may lead to requests for information from key investors, counterparties to financing arrangements, or potential parties to a corporate transaction. Disclosures of sensitive information to such parties may be necessary to minimize risks from the crisis. At the same time, a company should be careful that in making such disclosures, the strictures of Regulation FD are followed and additional issues are not created.

C. Voluntary Disclosure

Companies should carefully consider whether the disclosure of the existence of a government investigation is advisable even if such disclosure may not be required. One primary consideration is whether, if a company does not voluntarily disclose the existence of the investigation on its own initiative, such information will ultimately leak to the public—especially in the case of a cyberattack where personal information has been compromised by hacktivists who might be eager to disclose the information publicly—and to significant third parties, such as the company’s customers, suppliers and lenders. For example, the government could seek information from third parties, which might cause persons outside of the company to infer that an investigation is underway. In the event that questions do arise, a company must be careful not to falsely deny the existence of an investigation.

In addition, a company may conclude that it is better to disclose information about a potential issue earlier to acclimate the market and thereby minimize the risk of a strong reaction later. However, if this approach is taken, a company should be mindful of its duties to update the market. In particular, the company should always keep in mind that supplemental disclosure may be required if the litigation or investigation takes an unexpected turn. In this regard, it is important to evaluate whether the investing public is relying on prior disclosures concerning the existence of the litigation or investigation that may be misleading.

D. Practical Considerations

Once the existence of litigation or an investigation is disclosed, a company should consider the possibility of a deepening of the crisis, at least initially, including:
■ Other government or regulatory investigations;
■ Additional shareholder lawsuits;
■ An adverse impact on the company’s relationships with customers, suppliers, creditors, or business partners;
■ Concerns of employees, analysts, and shareholders; and
■ Unfavorable media coverage of the company.

Accordingly, as discussed in Section III, in advance of any voluntary and public disclosure, a company should be prepared for a resulting media response and inquiries.
IX. Conducting Internal Investigations

A complete discussion of the process and issues concerning an internal investigation is outside the scope of this InfoPAKSM. Nevertheless, there are aspects of a corporate crisis that impact the manner in which an internal investigation is supervised and conducted. For example, at the outset of a crisis, the crisis management team should ask:

- Will the company conduct an internal investigation to position itself to defend against government inquiries and private litigation?
- Will the company share information from its investigation with U.S. federal or state regulators in an attempt to secure credit for cooperation?
- Will the investigation lead to significant changes in senior management, such that external directors may be guiding the crisis response?

In light of the varied tacks that a strategy might take, it may be prudent for a company to pursue an initial approach that will maximize its flexibility and not foreclose any strategic responses. In contemplating such an approach, a company may consider how an internal investigation would be perceived by a skeptical government agency, litigant, or court at the end of the process. It may be useful to assess how best a company could persuade the government or a court that the findings of the internal investigation should be credited, and that the company acted appropriately upon learning of potential misconduct. As a general matter, a company maximizes its options by ensuring that any fact-finding and investigation are conducted in a full, fair, and forthright manner. Accordingly, company counsel should try to structure an internal investigation so that it is properly scoped and scaled, uses appropriate processes, and proceeds in an unbiased and untainted manner.

A. Defining the Proper Scope and Scale of the Investigation

Once it is clear that an internal investigation is warranted, and after the company decides who should conduct the investigation (whether inside counsel, outside counsel, or some combination thereof) and who will oversee the investigation (whether an independent committee of the board of directors or company officers), the responsible parties first should consider the scope of the investigation. If the scope of the investigation is drawn too narrowly, the government will distrust the investigation’s results, and the company will receive little credit for its efforts. If the scope is drawn too broadly, the investigation will become prohibitively costly for the company, and the delay in producing results may prove frustrating to the government and undermine the company’s credibility. To prevent unmet expectations, the company should consider communicating with relevant stakeholders (e.g., the government and auditors) at the outset of an investigation.

In determining how far to investigate, the company should be mindful that it will have to defend the investigation’s scope. For instance, the following non-exhaustive examples identify common questions that may be raised with respect to the investigation’s scope:

- Why did the company investigate some of its employees and not others, or some areas of its business and not others?
Did the company investigate the areas of its business most likely to present the greatest compliance risks?

Did the company perform any testing or analysis to determine if the misconduct was isolated or recurring in other regions?

Did the investigation examine whether the company’s most senior officials participated in or approved of the conduct?

How and why did the company limit the subject matter or time period of its investigation?

Did the investigation seek to interview individuals outside the company, such as former employees, agents or vendors, who potentially might have knowledge of the misconduct?

Did the investigation examine whether the company had a culture that permitted the misconduct to take place?

Did the investigation examine how the company’s internal controls and processes performed in detecting and preventing any misconduct?

Was the investigation conducted in a manner consistent with how other similar investigations have been conducted?

The proper scale of the investigation goes hand-in-hand with the proper scope of the investigation. It may be prudent for the company to consider making an early assessment of the alleged misconduct to determine the amount of resources to dedicate to the investigation. If the alleged misconduct is limited in nature, in-house counsel may be able to handle the investigation. However, if the alleged misconduct is global or widespread in nature, the company may want to engage outside counsel and forensic specialists. As the investigation progresses, the company should consider revisiting the scale of the investigation. Issues may arise that were not anticipated, and leads may develop that need to be pursued. Again, at the end of the process, the government is likely to ask a multitude of questions about the independence, thoroughness, and effectiveness of the investigation. For instance, did the company dedicate adequate resources to the investigation? Did the company engage specialists? When the company learned of additional misconduct, did it adjust the scope and scale of the investigation?

B. Establishing Appropriate Processes

At some point, the company will have to defend the processes used to conduct the investigation. Stakeholders will want to know how they can be reasonably confident that the investigation was thorough and that there will not be any new or surprising revelations after the investigation has been completed.

Did the investigation team develop a written protocol or work plan for the investigation?

What kind of information and documents did the investigators have when conducting the interviews?

Did the investigation rely on forensic accountants or other professionals to conduct an independent examination of the company’s books and records?
Two key areas that the government will examine are: (1) how the company identified the relevant documents and witnesses; and (2) how the company obtained relevant facts from witnesses, both of which are discussed in detail below.

I. Identifying Relevant Documents and Witnesses

Documents are usually a key part of most internal investigations. As noted in Section IV, it may be prudent for the company to identify and collect as early as possible relevant hard copy and electronic documents. Speaking to the company’s IT department and conducting preliminary interviews of relevant witnesses can help identify people who have knowledge of the custodians and the locations of important documents. The company will need to assure stakeholders that it located and preserved relevant documents.

- How did the investigation team identify, collect and examine all of the relevant documents?
- Did the investigation team consider other sources of documents and documents other than emails and electronic records (e.g., hard copy documents, storage rooms, mobile devices, etc.)?
- Did the investigation team use search terms and other parameters (e.g., date ranges) to search the company’s electronic documents and, if so, how did the investigation narrow the number of electronic documents reviewed?
- Did the investigation team revise the search terms based on the number of hits, new facts revealed, or if additional witnesses were identified?
- Should the investigation team utilize technology-assisted review (e.g., predictive coding software) if there is a large volume of documents?
- Should the investigation team undertake samplings before launching a full-scale review?
- Was a written record kept of the document search, collection, and review processes?
- Did the company send a document request and/or a preservation notice to relevant employees?
- To the extent witness interviews were conducted, did the interviewers ask the witnesses to provide any documents referenced during the interview, or any documents that potentially may be relevant to the investigation’s focus areas?
- Was a search conducted for documents outside the office (i.e., employees’ homes, publicly available news databases, and other sources of public information)?
■ If documents were located in a foreign country, did the company comply with local regulations (e.g., data privacy or state secrecy laws) when conducting the document collection and review processes?
■ Did the investigation team consider whether it needed translation services, and if so, whether those services should be provided by machines or professionals?

After the relevant documents are reviewed (or perhaps in certain circumstances before the relevant documents are reviewed), the company should identify relevant witnesses, both within the company and any relevant third parties, and begin conducting interviews. The company will need to assure stakeholders that it identified relevant witnesses.

■ Did the company identify key witnesses early in the investigation?
■ What resources did the company use to identify relevant witnesses?
■ Did the company identify relevant witnesses who are former employees or third parties?
■ Did any witness identify other witnesses that may have knowledge, but were not previously identified by the company?

2. Conducting Effective Interviews

Interviews are a critical aspect of a successful internal investigation. The company will need to assure stakeholders that it effectively interviewed all relevant witnesses. In preparing an interview plan, the company should address key issues, such as:

■ Are there any topics or areas which may necessitate consulting the company’s policies and procedures in advance of conducting interviews on those topics?
■ Are there any local laws that should be considered before conducting interviews in foreign locations?
■ In what order should the relevant witnesses be interviewed?
■ Should the interviews be conducted in person, by telephone, or by video conference, and what are the benefits and limitations of each method? If in person, where should the interviews take place?
■ Who should be present at the interviews?
■ Do any of the interviews require the presence of interpreters?
■ Will the witness be permitted to review relevant documents before the interview?
■ Does the witness need to have personal counsel?
■ Should the company indemnify or advance to the witness reasonable fees and expenses associated with the participation of personal counsel?
■ Did counsel give the witness “Upjohn warnings?”
■ Who will take notes and by what method will the notes be taken?
■ Should formal interview memoranda be prepared by counsel? If so, what should the memoranda include?
Should the interview memoranda be shared with the witnesses?

C. Ensuring an Unbiased Approach

Ultimately, the company will have to show that its investigation was open to pursuing facts showing misconduct, wherever that might lead. For instance, the company should expect the government to assess:

- How thorough was the questioning of the witnesses?
- To what extent did the investigation corroborate the information learned in the witness interviews?
- At the conclusion of the interviews, did the investigators ask witnesses the catch-all question of whether they had any other concerns or issues, ethical or otherwise, about any conduct within the company, regardless whether it was related to the investigation?
- If so, did the investigators pursue any leads suggested by the witnesses?

D. Providing Untainted Analysis

Likewise, the government also will need to know that the fact-finding process in the investigation was not tainted in any way. For instance:

- Did any witness in the investigation have any control over how the investigation was conducted or have any way of learning the results of the investigation?
- Were witnesses admonished to maintain the confidentiality of their interviews?
- Were there any opportunities for witnesses to coordinate their stories?
- Did a witness, in a supervisory position, influence other witnesses’ responses?

E. Documenting Findings and Conclusions of Investigation

It may be prudent for the company to have counsel prepare a report documenting the findings and conclusions of the investigation. The content and form of the report will depend on the seriousness of the conduct at issue and the intended purpose of the report. The stakeholders will need to know that the company conducted a thorough investigation and took remedial actions to correct any wrongdoing.

- What level of detail should be included in the report?
- What style and tone should be used?
- Is the report tailored to the relevant constituency?
- Should comments be solicited?
- Is the report fair and balanced—it neither exaggerates the evidence nor minimizes it?
■ Does the report include the company’s remedial actions?
■ Does the report avoid sweeping pronouncements?
■ Does the report tell the story clearly, concisely, accurately, and chronologically?
■ What is the form of the report (e.g., full written report, presentation slides, oral report, etc.)?
■ If disclosing findings to the government, did the company identify and disclose all relevant facts regarding individuals’ misconduct to receive credit for cooperation?133

As noted in Section VII.C., a decision will need to be made whether the report should be in written or oral form. The answer to this question will depend upon the circumstances presented. Written reports can offer a number of benefits, including substantially more content and more precise analysis, and they are often easier to digest than an oral report. But written reports carry the risk that they may become discoverable. If the risk of private civil litigation is significant, the company will need to weigh the costs and benefits of preparing a detailed written report. Additionally, the form of the report may depend on the regulators involved. Certain foreign government regulators want a complete written report upon the completion of an investigation.

There is no one-size-fits-all internal investigation. The answers to many of these questions are fact-specific. What might be perfectly reasonable in one situation—and perfectly defensible to the government—might be patently unreasonable and indefensible in another. Not every situation requires a full-blown internal investigation. The end result, however, should be the same: the company wants to be in a position where it has earned credit from the government for conducting an impartial, thorough, and accurate investigation, which is appropriate for the circumstances and which produces results upon which the company and the government can reasonably rely.
X. Minimizing Privilege Waivers

As highlighted in many of the sections above, the issue of privilege waiver arises frequently in the context of parallel proceedings. In particular, whenever a company voluntarily discloses privileged material as part of a cooperative approach with a government entity, the company must consider whether the disclosure will constitute a waiver of attorney-client privilege or work product protection over those documents (or possibly other documents on the same subject matter) in other proceedings. Although less commonly litigated, privilege waivers also can arise through intra-company communications made during the course of parallel proceedings, or through disclosure in shareholder litigation or civil settlements where other proceedings are pending. Finally, with the increasing prevalence of cross-border investigations, companies should be sensitive to variations in the scope and nature of the privilege between different jurisdictions. This section addresses each of these circumstances in turn.

A. Government Investigations

1. Attorney-Client Privilege

As previously noted, in deciding whether criminal prosecution is appropriate, the DOJ considers a corporation’s timely and voluntary disclosure of wrongdoing. Eligibility for such cooperation credit generally is not predicated on the disclosure of privileged information. Nevertheless, a company must disclose “all relevant facts” in order to receive credit. Because a considerable amount of information acquired during an internal investigation may implicate the attorney-client privilege and attorney work product protection, a company may conclude that it is advisable to voluntarily disclose privileged material in some circumstances.

Courts in the United States have adopted divergent positions on whether, and to what extent, voluntary disclosure of attorney-client privileged material in the course of a government investigation may waive the privilege in subsequent or parallel proceedings. The U.S. Court of Appeals for the Eighth Circuit, in Diversified Industries v. Meredith, held that a company could voluntarily disclose attorney-client privileged material in response to a request by an investigating government agency without thereby waiving the privilege in a parallel civil proceeding. However, most other circuits that have addressed this concept of “selective waiver” in the context of government investigations have rejected the reasoning of Diversified, citing the inherently adversarial relationship between the government and the regulated party, and concluding that selective waiver would not serve the purposes underlying the attorney-client privilege to encourage full and frank communication between attorneys and their clients.

A few courts—notably the U.S. Court of Appeals for the Second Circuit in In re Steinhardt Partners, L.P.—have suggested that the use of a sufficiently restrictive confidentiality agreement or other circumstances may prevent waiver. However, lower courts in the Southern District of New York have reached dramatically different conclusions following Steinhardt, with some upholding the privilege where the disclosing party had entered into a
confidentiality agreement that explicitly limited disclosure to the government investigating agency, and others identifying the Second Circuit’s holding as dicta and admonishing that such selective waiver could easily be abused and manipulated to gain tactical or strategic advantage.\(^{139}\) Other courts—notably the U.S. Court of Appeals for the Ninth Circuit in In re Pacific Pictures Corp.—have flatly rejected a post-disclosure confidentiality agreement between a private party and a government agency, concluding that there is nothing to suggest that such agreements would “encourage frank conversation at the time of the advice.”\(^{140}\)

In addition to carefully considering this divergent case law, a company contemplating a “non-waiver” agreement with a government agency should review Federal Rule of Evidence 502 (“FRE 502”), which offers guidelines for examining party agreements. For example, FRE 502(e) states initially that agreements on the effect of disclosure in a federal proceeding are binding only on parties to the agreement. This does not appear to affect the waiver analysis of the courts above, and federal courts generally have continued to analyze waiver based on disclosure to government agencies by analyzing the terms of confidentiality agreements.\(^{141}\) At the same time, however, FRE 502(e) states that party agreements on waiver and disclosure may bind third parties if the agreements are incorporated into a court order. FRE 502(d) complements this provision, providing that when a confidentiality order governing the consequences of disclosure in that case is entered in a federal proceeding, its terms are enforceable against non-parties in any federal or state proceeding.\(^{142}\) Thus, FRE 502(d) and (e) allow a court to incorporate agreements into orders or issue orders regarding the waiver of privilege in litigation pending before the court, and these orders are binding in any other federal or state proceeding.

Regarding the structure of orders under FRE 502, the Rule itself contemplates a broad range of possibilities, but courts have introduced uncertainty. Some courts have issued orders pursuant to FRE 502 that limit waiver for both inadvertent and intentional disclosures by parties.\(^{143}\) Other courts have incorporated a reasonableness element into the analysis of a party’s agreement under 502(d),\(^{144}\) despite the language of the Committee Notes that encourages orders limiting waiver “irrespective of the care taken by the disclosing party” and including “claw-back” and “quick-peek” provisions.\(^{145}\) Where courts have incorporated a reasonableness requirement into their analysis of party agreements, they have typically drawn it from another section of FRE 502 that deals with inadvertent production, FRE 502(b).\(^{146}\)

2. Work Product

U.S. rules governing selective waiver of work product generally overlap with those governing attorney-client privilege. For example, federal circuits generally hold that the production of fact work product to a government agency waives work product protection, but there remains, subject to the provisions of FRE 502(d) and (e), a split in authority over whether a confidentiality agreement can change that outcome.\(^{147}\) Moreover, courts have diverged over whether to distinguish selective waiver of opinion work product (revealing attorney mental impressions and legal theories) from selective waiver of fact work product (such as chronologies or factual summaries).\(^{148}\) FRE 502 itself makes no such distinction, but several courts have differentiated between opinion work product and fact work product when determining the scope of subject matter waiver under FRE 502 based, to some extent, on Federal Rule of Civil Procedure 26(b)(3)(B)’s special protection “against
disclosure of the mental impressions, conclusions, opinions, or legal theories of a party’s attorney or other representative concerning the litigation.”\textsuperscript{149}

3. **Subject Matter Waiver**

Until the passage of FRE 502, courts generally had rejected efforts at “limited” or “partial” disclosure, where a party discloses one portion of privileged material but not the remainder on the same subject matter. For example, several court rulings had held that production of a privileged report to the government could constitute waiver of privilege or work product protection as to both the report and any underlying supporting documents, even if the underlying documents were never requested by or produced to the government.\textsuperscript{150} FRE 502, however, provides guidelines for courts to follow in analyzing subject matter waiver. Specifically, FRE 502(a) sets up a three-part test for determining when a disclosure made in a federal proceeding or to a federal office or agency waives the attorney-client privilege or work-product protection for an undisclosed communication or information in the proceeding or another federal or state proceeding. The waiver must be intentional, the disclosed and undisclosed communications or information must concern the same subject matter, and the court must find that the undisclosed materials ought in fairness to be considered together with the disclosed materials. Courts have interpreted the third prong of the test, whether the undisclosed materials ought in fairness to be considered with the disclosed materials, in a way that generally excludes opinion work product.\textsuperscript{151}

In *Mitre Sports International, Ltd. v. Home Box Office, Inc.*, the Southern District of New York declined to find subject matter waiver where the disclosure was not designed to influence a decision maker.\textsuperscript{152} In *Mitre*, the defendant sought access to documents concerning an internal investigation conducted by the plaintiff, arguing that it had relinquished privilege by allowing an investigator to testify regarding certain aspects of the investigation and attaching the products of its investigation to its complaint.\textsuperscript{153} Citing the Advisory Committee notes to FRE 502, the court concluded that there was no subject-matter waiver where (i) the plaintiff did not rely on the investigator’s testimony regarding the protected material and (ii) the investigation was not relevant to any of the remaining issues in the action. The court distinguished these facts from those where disclosure was made to persuade a regulator that “no violation of the securities laws had occurred” or materials were discussed in trial testimony “in an effort to influence a decision maker.”\textsuperscript{154} The court’s holding thus suggests that a different outcome may have resulted had the party furnished the results of its investigation to a regulator.

Given the potential for a finding of privilege waiver when information is shared with the government, a number of practical considerations may factor into the extent and manner in which privileged material is disclosed in parallel proceedings:

- The company should consider the extent to which it can cooperate with a government investigation through the provision of non-privileged information;
- The company should consider the purpose underlying production of certain documents (i.e., persuading the government to forego enforcement vs. providing general background information regarding the company’s operations);
■ The crisis management team should understand the import of the information being generated to all pending proceedings in order to coordinate production and ensure that steps are taken to reduce privilege waivers as appropriate; and
■ When a company decides to disclose privileged information to the government, the company should request a confidentiality agreement that includes:
  • Incorporating the agreement into a controlling court order that will bind third parties;
  • Express limitations on the investigating agency’s use of the privileged material to resolution of the investigation at issue;
  • Provisions allowing the “claw-back” and “quick-peek” provisions mentioned in the Committee Notes;
  • Provisions requiring the agency to undertake specific steps to ensure that the confidentiality of the material is maintained, including segregating the material from other non-privileged documents, filing the material under seal, maintaining records of the material’s use, or otherwise handling the material in a special way;
  • Provisions indicating that, if the agency must disclose the material as required by law, the agency will notify the disclosing company;
  • Provisions requiring the agency to maintain the confidentiality of the materials in a manner that exempts them from disclosure under the Freedom of Information Act or similar state statutes; and
  • Provisions indicating that the disclosure will not be considered a privilege waiver, either for any related subject matter or any third parties.

B. Intra-Company and Common-Interest Communications

Additional privilege waiver issues arise in the context of parallel proceedings because of dissemination of information about internal investigations within a company. For example, in Ryan v. Gifford, the Delaware Chancery Court addressed a situation in which a company, faced with a derivative action concerning allegations of stock-options backdating, established a special committee comprised of the company’s sole disinterested board member to conduct an internal investigation and present a report to the company’s full board of directors. When the plaintiff shareholders in the derivative action sought to compel production of the report and underlying investigative materials, the company resisted on grounds of attorney-client privilege and work product protection.

The court held that the presentation of the results of the investigation to the full board of directors waived the attorney-client privilege as to all communications relating to the investigation. The court based this ruling on two points: first, that the individual directors, who were accompanied by personal counsel at the board meeting at which the report was presented, were third parties for purposes of waiver, and second, that there was no common interest between the individual directors and the special committee. The court thus characterized the relationship between the special committee and the directors as adversarial, noting that the special committee was established to investigate wrongdoing.
Although it remains to be seen whether other courts will follow the Ryan court’s lead, certain practical steps may be taken to minimize the risk of waiver as a result of intra-company disclosure:

- Consider limiting dissemination of the results of an internal investigation to individual employees on a “need-to-know” basis;
- Consider requesting that individual officers or directors who are potentially involved in the subject matter underlying the investigation recuse themselves from discussions about the investigation;
- Consider prohibiting individual counsel for officers or directors from attending discussions about the investigation; and
- Consider entering into a joint defense or common interest agreement with officers or directors, as appropriate.

Companies should take particular care in considering whether to enter into a joint defense or common interest agreement with individual officers or directors who may be directly implicated in improper conduct. The privilege may be asserted so long as the parties to the agreement have a common legal interest or are involved in a “joint defense effort or strategy,” even when they are not presently involved in ongoing litigation. However, the parties must share a “common legal interest” as opposed to a “common business interest” for the privilege to apply.

The common-interest or joint defense agreement also may be used to avoid waiver of communications between different companies involved in a government investigation. With respect to such inter-company communications, the best course may be to refrain from any disclosures unless a common legal goal may be identified and, though not necessary, it may be advisable to enter into a specific joint-defense agreement prior to the disclosure of any confidential information. While this goal need not arise in the context of ongoing litigation, the parties must have a stake, beyond mere commercial interests, in the same resolution to a legal question.

Moreover, the common interest privilege has certain limitations. Specifically, the privilege only extends to communications made during the period when the parties shared a common interest. In other words, communications taking place before the parties’ interests aligned are not protected, nor are communications made after the parties no longer share a common interest. However, although communications post-dating the common interest have no protection, it is not the case that “communications that occurred during the time their common interest existed . . . later los[e] their privileged status.” These temporal constraints underscore the importance of documenting, prior to any disclosure, the existence of a joint strategy. This places potential litigants in a difficult position where certain disclosures may be necessary to determine whether a third party does, in fact, share a common goal.

C. Parallel Shareholder Lawsuits and Civil Settlements

Further issues of privilege waiver may arise in the context of parallel proceedings where privileged information is disclosed first in the course of a derivative lawsuit pursuant to Garner v. Wolfinbarger, and is simultaneously or subsequently sought in other civil
litigation or government proceedings. Such circumstances may raise an issue as to whether disclosing materials under court order to shareholders in a derivative action waives the privilege over them as to any subsequent litigant. One U.S. federal court of appeals to have addressed this issue, the U.S. Court of Appeals for the Sixth Circuit, has held that a disclosure made pursuant to Garner can be maintained under seal in the derivative action, thus preserving the confidential and privileged nature of the materials as against future litigants. Another federal court of appeals, however, the U.S. Court of Appeals for the Second Circuit, has held that placing the privileged disclosure “at issue” in a derivatives action waives all privilege.

In addition, although selective waiver is generally addressed in situations in which an initial disclosure is made to a government investigator, it has the potential to become an issue in any instance where a disclosure is made in one of several parallel proceedings. For example, in the case of In re Chrysler Motors Corp., the court held that by disclosing attorney work product in the course of a class action settlement proceeding, even under a confidentiality agreement, the company waived work product protection over the material in a criminal sentencing proceeding.

Of course, FRE 502(d) and (e) present the possibility of avoiding uncertainty by seeking a court order to determine the effect of disclosure on privilege or protection in other federal and state proceedings. Indeed, the litigation context squarely fits with the purpose of FRE 502, which was to reduce production costs. FRE 502 also offers protections to a party in a state action since FRE 502(c) limits waiver in a federal proceeding where disclosure is made in a state proceeding and the disclosure either would not be a waiver under FRE 502 or would not be a waiver under the law of the state where the disclosure occurred. This is limited, however, to situations where the state court has not issued an order concerning waiver. Accordingly, in any matter where there is a potential for parallel proceedings to arise, it is advisable for a company to be able to assess comprehensively at the outset, the impact of disclosing or withholding privileged material across multiple proceedings, as well as the potential benefit of seeking a court order stating the effect of disclosure on privilege or protection. Parties seeking an agreement during litigation can take certain practical steps to minimize the risk of waiver as a result of disclosure:

■ Consider incorporating the agreement into a controlling court order that will be binding on third parties;
■ Consider drafting the agreement in a way that explicitly defines its scope, including whether it will apply to both inadvertent and intentional disclosures or whether it will include privilege and work product protections; and
■ Consider drafting the agreement in a way that will avoid any “reasonableness” review that a court may impose, including spelling out the need for any questionable provisions, such as the cost savings of any “claw back” or “quick-peek” provisions, and explicitly detailing the workings of these provisions.

D. Cross-Border Investigations

With companies increasingly subject to inquiries and investigations by regulators and law enforcement agencies from multiple jurisdictions around the world, it is more important than ever to be vigilant of the varying consequences of disclosure under different legal
regimes. While most countries recognize some form of attorney-client protection, the privilege rarely overlaps completely with that of the United States. Counsel also should be aware of differences in ethical rules governing how attorneys treat a client’s documents and communication, including disclosure.

Common law countries generally shield communications between lawyers and clients that relate to the clients’ legal positions. For example, the United Kingdom recognizes two types of privilege that will sound familiar to American attorneys: legal advice privilege and litigation privilege. Legal advice privilege, which is not unlike the attorney-client privilege, extends to communications with all attorneys, including in-house counsel, in which the client seeks legal advice. On the other hand, the litigation privilege applies when adversarial proceedings are reasonably imminent and covers work product and (some) third-party communications so long as their “dominant purpose” is the provision of legal advice.

Civil law countries, by contrast, usually provide a statutory basis for the privilege and require litigants to produce only those documents on which they intend to rely at trial. The European Union, for example, recognizes legal privilege as a fundamental right by the European Court of Justice. It should be noted that this right generally may not extend to in-house counsel, which are deemed to be lacking “independence” from their employer. In non-European jurisdictions, the attorney-client privilege may be even narrower or entirely absent. In China, for example, government authorities or the court may compel a lawyer to disclose client confidences or work-product. Japan likewise does not have a specific attorney-client privilege, although Article 197(2) of its Code of Civil Procedure, as amended in 1998, allows a lawyer to refuse to testify where the lawyer “is questioned with regard to [a] fact [of] which he has obtained knowledge in the exercise of his professional duties and should keep secret.” A similar protection exists for documents fitting this description.

With the above complexities in mind, companies currently engaged in, or facing the possibility of engaging in, cross-border investigations should consider the following practices:

■ Understand the privilege laws in the applicable jurisdiction(s).
■ Consider retaining competent local outside counsel in the relevant jurisdictions.
■ Ensure that written communications are labeled as privileged and/or confidential, including using the phrase in the local language.
■ Limit access to privileged materials in jurisdictions with extremely limited or non-existent privilege.
■ Ensure that internal investigations are conducted at the direction of counsel, even if non-attorneys conduct day-to-day investigation activities.
XI. Anticipating Employee Issues

Crises frequently present counsel with a variety of employee-related issues that also must be considered by the crisis management team. These issues include how to address the legal representation of employees, what steps it should take in the event an employee’s conduct is called into question, and how it should deal with “whistleblower” situations. Although a company may have a fair amount of discretion in deciding how to deal with these issues, counsel must be mindful of limitations and requirements imposed by employment contracts, corporate bylaws, conflict of interest guidance, labor and employment laws, and regulations and guidance by regulatory agencies. Indeed, a recent memorandum from the DOJ has garnered much attention from the white collar bar as it evidences an increased focus of the civil and criminal authorities on culpability of individuals, including corporate officers and employees.

A. Legal Representation of Employees

1. Upjohn Warnings

As explained in Section IX, employee interviews are a fundamental component of any internal investigation conducted in the wake of a crisis. Interviews of employees knowledgeable about the incident will help the company determine what happened, why it happened, who else was involved, how to address the problem, and how to prevent it from occurring again. If properly conducted by company counsel so the attorney can provide legal advice to the company, employee interviews generally should be protected by the company’s attorney-client privilege. It is critical, however, that company counsel make clear to the employee that they are attorneys for the company, not the employee, and that the company alone therefore has the right to decide whether to waive or assert the privilege with respect to the statements that the employee makes during an interview. Thus, counsel should provide the full Upjohn warnings, also known as the “corporate Miranda warnings,” at the outset of every employee interview, ensure that the employee understands the warnings and memorialize it in writing.173

Failure to provide adequate Upjohn warnings during an employee interview could have serious consequences for both the company and its counsel. If the employee is left with the reasonable belief that the attorneys conducting the interview are representing his or her interests, a court may conclude that the attorney-client privilege applies to both the company and the employee.174 In such a scenario, the employee would be able to prevent the company from disclosing information that the employee imparted during the interview.175 A company cooperating with the government may find itself in a predicament if an employee admits his involvement in wrongdoing and later blocks the company from disclosing this information to the government. Moreover, to the extent that a court finds that company counsel represents both the company and the employee as the result of providing inadequate Upjohn warnings, company counsel involved in making disclosures to the government about the employee’s admissions could find himself subject to an ethics complaint for breaching his duty of loyalty to the employee.176
2. **Separate Legal Representation**

In general, companies may provide separate representation for employees who are called as witnesses or named as defendants during parallel proceedings arising out of a crisis.\(^{177}\) Company counsel may wish to provide separate counsel to ensure that employees receive adequate advice and preparation in connection with such matters. Separate counsel may help not only the employees but also the company in ensuring that facts are thoroughly investigated and clearly presented and that legal and business considerations are appropriately analyzed and implemented.

A similar issue is whether a company should retain a single firm to represent all employees in need of representation. A company may choose to use a single firm for all employees to reduce fees and to leverage counsel’s factual knowledge, but joint representation can lead to complex conflict of interest issues, particularly if conflicts arise between the employees being represented.\(^{178}\) In addition, the SEC’s “sequestration rule” seeks to restrict cross-representation of multiple witnesses by counsel;\(^{179}\) however, the courts have responded to this rule with disfavor.\(^{180}\)

To enable its employees to retain high quality and experienced counsel, a company will generally be permitted, and may be required, to indemnify or advance funds for employees’ attorney fees and other related expenses. A company may be required to provide indemnification or fee advancement under state law, its own bylaws or partnership agreements, or the employment contracts of the employees in question.\(^{181}\) Also, companies might exercise their business judgment to offer these benefits as part of a strategy to attract and retain high quality employees in industries that may face potential legal risks.

The fact that a company pays an employee’s attorney fees does not necessarily result in a conflict of interest for the attorney. The United States Supreme Court, however, has indicated that a conflict of interest may result if “counsel was influenced in his basic strategic decisions by the interests of the employer who hired him.”\(^{182}\) Company counsel should accordingly avoid influencing or attempting to influence an individual employee’s attorney, in order to avoid allegations that a conflict of interest deprived the employee of his right to independent and zealous representation.

The Thompson Memorandum,\(^{183}\) which was issued by the DOJ in 2003 and addressed federal prosecution of business organizations, discouraged companies from paying for employees’ legal representation by singling out indemnification as one of several factors that prosecutors could consider in determining whether to bring federal charges against a company. Following criticism of this approach, the DOJ issued the McNulty Memorandum\(^{184}\) in 2006 and the Filip Letter\(^{185}\) in 2008. Incorporating those pronouncements, the USAM chapter on Principles of Federal Prosecution of Business Organizations now specifies that “[i]n evaluating cooperation, however, prosecutors should not take into account whether a corporation is advancing or reimbursing attorneys’ fees or providing counsel to employees, officers, or directors under investigation or indictment.”\(^{186}\) The USAM further notes that prosecutors may not request that companies refrain from paying employees’ attorneys’ fees.\(^{187}\) These changes are consistent with the August 2008 decision of the U.S. Court of Appeals for the Second Circuit in *United States v. Stein*,\(^{188}\) which affirmed the dismissal of indictments against KPMG partners and employees. *Stein* held that pressure from prosecutors while KPMG was seeking cooperating credit affected
KPMG’s decision whether to pay individuals’ attorneys’ fees and violated the individuals’ Sixth Amendment right to counsel of their choice.\textsuperscript{189}

As discussed in other sections of this publication, the Yates Memorandum directs the DOJ to “focus on individual wrongdoing from the very beginning of any investigation of corporate misconduct.”\textsuperscript{190} Accordingly, the need to consider providing counsel for employees becomes even greater. As a result, when trying to attract executives or other top talent, companies must consider the value in providing indemnification provisions or promising to cover legal costs in an executive’s employment contract. Additionally, companies should consider whether any director and officer insurance policies contain appropriate coverage for any applicable defense costs.

\section*{B. Discipline}

In the course of parallel proceedings, a company’s own fact-finding efforts or those of outside parties may reveal that an employee has engaged in questionable conduct. In this situation, the company must consider what steps, if any, to take with respect to that individual’s employment. As described below, government policies provide strong incentives for disciplining or dismissing an employee who has engaged in wrongdoing. These decisions, however, may be tempered by considerations such as the employment agreements of the individual in question, labor and employment laws in the relevant jurisdictions, the procedural stage of the government proceedings, and whether wrongdoing has been proven against the employee.

The SEC’s 2001 “Seaboard Report”\textsuperscript{191} contained guidance on how the SEC evaluates a company’s remediation and cooperation efforts. Among the criteria the SEC will consider are the steps the company took when it learned of the misconduct, and whether individuals responsible for the misconduct are still employed by the company and in the same positions.\textsuperscript{192} Prior to 2008, DOJ guidance indicated that a company’s failure to discipline employees for known misconduct could influence the government in its assessment of the company’s level of cooperation with the government’s investigation. The McNulty Memorandum viewed a company’s failure to discipline an employee as an indication of uncooperativeness.\textsuperscript{193} The Filip Letter amended that position, stating:

\begin{quote}
Federal prosecutors will not consider whether the corporation has retained or sanctioned employees in evaluating cooperation. How and whether a corporation disciplines culpable employees may bear on the quality of its remedial measures or its compliance program; it will not be taken into account for the purpose of evaluating cooperation.\textsuperscript{194}
\end{quote}

In revisions to the USAM in August 2008 as a result of the McNulty Memorandum and the Filip Letter, the DOJ specified that, when evaluating the company’s degree of cooperation, federal prosecutors are no longer permitted to consider whether a corporation has disciplined or terminated implicated employees. The USAM notes, however, that a prosecutor may consider remedial measures, including whether a corporation has disciplined culpable employees, “in determining whether to charge the corporation and how to resolve corporate criminal cases.”\textsuperscript{195} In addition, whether a corporation has taken disciplinary
action against culpable employees can be considered in determining the effectiveness of a corporation’s compliance program.196

Further, the U.S. Sentencing Guidelines Manual, last revised as of November 2015, states that a company must consistently enforce its compliance and ethics program through “appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.”197

For example, in connection with DOJ charges against IAP Worldwide Services, Inc. for violating the Foreign Corrupt Practices Act, the DOJ agreed to a non-prosecution agreement between the DOJ and the company. In reaching the agreement, the DOJ recognized that IAP had “engaged in remediation, including disciplining the officers and employees responsible for the corrupt payments or terminating their employment.”198 Similarly, in a 2013 case, the SEC announced that it had declined to take enforcement action against Ralph Lauren Corporation because of its “extensive, thorough, real-time cooperation” with the SEC’s investigation.199 The SEC highlighted the fact that Ralph Lauren terminated its customs broker responsible for the misconduct.200

When contemplating disciplinary action, company counsel should analyze:

- Whether an employee received a financial or other advantage from the conduct;
- Whether the conduct was the result of error or misunderstanding or was planned or deliberate;
- Whether the conduct occurred once or multiple times;
- Whether the employee received training, notice or warnings about the conduct; and
- Whether the employee cooperated with the investigation or otherwise came forward to address the situation.

C. “Whistleblower” Protections

In the context of a crisis, a company must be particularly sensitive to actions taken with respect to employees who report or otherwise draw attention to alleged wrongdoing within the company. Such reports may be made to company personnel, government regulators or other third parties, including independent auditors or even outside counsel.201 Various U.S. federal and state laws provide protections and monetary incentives for so-called whistleblower employees to report alleged wrongdoing. For example, the Dodd-Frank Act protects employees who report potential violations of laws enforced by the Consumer Financial Protection Bureau,202 as well as potential violations of the securities and commodities laws.203 Additionally, tips that lead to an enforcement action by the Securities and Exchange Commission or the Commodity Futures Trading Commission (CFTC) resulting in sanctions of more than $1 million entitle informants to collect bounties of between 10% and 30%.204 Similarly, under the False Claims Act (FCA), whistleblowers can recover bounties in certain cases involving federal government spending.205 These laws and others like them dovetail with government programs that hold out the prospect of non-prosecution or diminished charges for individuals who provide information about illegal activity and cooperate with government investigations.206 In recent years, the government
has increasingly relied on whistleblowers for recoveries, and the SEC has issued awards to individual whistleblowers of $5 million, $14 million, and $30 million. Moreover, in fiscal year 2015, the DOJ reportedly paid out $597 million to qui tam relators.

In general, companies should take employees’ allegations of wrongdoing seriously by promptly and thoroughly investigating and addressing them. Where a company has reason to believe that an employee has already provided or may provide information to the government, the company should consider informing the government of the results of its investigation and any steps taken by the company to address its findings. A company is likely to find itself in greater difficulties for ignoring so-called “whistleblower” allegations or treating them superficially, than if the allegations had been dealt with properly, particularly in light of the importance that DOJ and SEC guidance place on companies’ responses to reports of wrongdoing. Moreover, because the law gives employees strong incentives to report perceived or potential misconduct, thereby depriving the company of the opportunity to control the circumstances under which the government learns of such issues, companies should assume that the period of time during which a crisis can remain confidential is limited.

The broad purpose of “whistleblower” laws is to encourage employees to come forward without fear of facing disciplinary measures at work or losing their jobs. In some cases, legal protections for employees who report alleged misconduct may even stand in tension with the need to discipline culpable employees, discussed above. Companies must proceed with great caution when considering termination, discipline, or any other action that might be construed as retaliation against an employee who has alleged wrongdoing, even if the reasons for the potential employment action are unrelated to the allegations.

Incentives and protections for employees to report alleged misconduct to the government highlight the need for companies to develop or reinforce effective and well-known internal compliance programs. Company policies should encourage employees to report potential misconduct internally, and potential misconduct should be quickly and appropriately escalated internally. Ideally, employees will feel comfortable reporting any perceived issues internally, giving companies time to fully investigate and address such issues. Additionally, employee evaluation and disciplinary procedures should ensure that the company’s reasons for taking specific employment actions are clearly and adequately documented.

Companies may include confidentiality, cooperation and waiver provisions in employee agreements to limit an employee’s options if he or she fails to maintain confidentiality, report suspected violations to a supervisor internally, or cooperate in an investigation. Any such agreement cannot force the employee to indemnify the company for FCA liability, but some courts have allowed an FCA defendant to pursue a claim against the employee for independent damages where (i) the conduct at issue is distinct from the conduct underlying the FCA case or (ii) the defendant’s claim can only prevail if the defendant is not found liable in the FCA case.

Recent SEC regulations, however, have complicated certain of these provisions and should be considered by public companies when conducting internal investigations. SEC Rule 21F-17, enacted pursuant to the Dodd-Frank Act, protects individuals who provide information regarding potential violations of the securities laws to the SEC. In its first enforcement action under the rule, the SEC instituted settled administrative proceedings
against KBR, Inc., alleging that the company required employees involved in an internal investigation to sign confidentiality agreements warning that they could be disciplined or fired if they discussed the subject matter of the investigation without prior approval. In a press release, the SEC stated that such agreements “may silence potential whistleblowers before they can reach the SEC.” KBR agreed to pay a $130,000 penalty and amend its confidentiality agreement to resolve the matter.

D. Practical Considerations

Below are practical tips for company counsel in dealing with employment issues that may arise in the context of parallel proceedings following a crisis.

- Review relevant employment contracts, company human resources policies and applicable state and federal labor and employment laws, and potentially consult with employment counsel sensitive to the risks inherent in crisis-induced parallel proceedings, to identify and understand:
  - The company’s indemnification obligations toward employees who may be involved in the proceedings;
  - Disciplinary options if employee conduct should prove to be an issue; and
  - Whistleblower protections if employees have made allegations of wrongdoing.

- Consider whether employees involved in the parallel proceedings should retain separate counsel.

- If so, consider identifying competent counsel and assisting in arranging the representation.
XII. About the Authors

This InfoPAK was authored by Gary DiBianco, David B. Leland and Paul A. Solomon of Skadden, Arps, Slate, Meagher & Flom LLP. For additional information on Skadden, Arps, please visit their website at http://www.skadden.com.

Gary DiBianco is a partner in Skadden’s Washington, D.C. Litigation and Government Enforcement Group. He specializes in white collar defense and securities and consumer fraud class action cases. He represents a broad array of clients in civil and criminal government investigations and complex civil litigation in matters involving federal and state securities laws, the accounting and anti-bribery provisions of the U.S. federal Foreign Corrupt Practices Act (FCPA), consumer protection statutes, and federal and state false claims acts. Mr. DiBianco’s clients include U.S. and foreign companies, financial institutions, accounting firms and individuals. He has advised and represented audit committees, boards and special litigation committees in connection with government investigations and shareholder litigation. Many of his matters involve simultaneous federal and state investigations and civil proceedings.

David Leland is also a partner in Skadden’s Washington, D.C. Litigation and Government Enforcement Group. He represents corporations, officers, directors and employees in connection with criminal, civil, administrative and congressional proceedings. His practice focuses on white collar criminal defense, complex civil litigation and SEC enforcement actions at all stages, from investigation through trial. He has defended corporations and individuals in the United States and abroad against allegations of Foreign Corrupt Practices Act violations, tax evasion, false claims, government procurement, mail and wire fraud, false statements, computer fraud, bank fraud, trade sanctions and securities fraud violations. He conducts internal investigations on behalf of major corporations, boards of directors and audit committees. As a former senior congressional aide, Mr. Leland also advises clients on congressional investigations and legislative matters.

Paul Solomon is a counsel in Skadden’s Washington, D.C. Litigation and Government Enforcement Group. He represents corporations and their audit committees, officers, directors and employees in connection with a wide variety of investigations conducted by the DOJ, SEC, and other federal and state law enforcement agencies. Mr. Solomon’s practice focuses on white collar criminal defense, complex civil litigation and enforcement actions. He has defended corporations against allegations arising under the U.S. Foreign Corrupt Practices Act (FCPA) and the False Claims Act, as well as actions based upon federal mail and wire fraud statutes and federal securities fraud. Mr. Solomon has extensive experience conducting global investigations and compliance reviews, including matters in more than twenty countries in Africa, the Americas, APAC and Europe.

The authors would like to thank Jen Spaziano, Margaret Krawiec, Bruce Macaulay, Nick Adams, James Altman, Robyn Baggetta, Mike Bailey, John Barkmeyer, Cory Black, Michelle Bosworth, Mike Burns, Gina Cardenas, David Carney, John Coghlan, Frank Correll, Jen Gindin, Nicole Grimm, Yeney Hernandez, Paul Kerlin, Vicki Kinne, Kate Lesker, T.J. Parnham, David Pehlke, Erica Perdomo, Gary Rubin, Dan Sullivan, Sherry Tao, and Ed Williams, for their assistance in researching and drafting the content of this article.
XIII. Additional Resources


For more ACC InfoPAKs, please visit http://www.acc.com/infopaks


XIV. Appendices

A. Crisis Management Plans: Operational Checklist

- Create a Crisis Management Plan
  - Identify crisis management team members and stakeholders to form a crisis management or “rapid response” team; appoint a team or project leader, spokesperson and role players.
  - The plan also should classify incidents, establish protocols to determine who should be notified, how to document, investigate and remediate incidents.

- Provide training to members of the crisis management team.

- Within the first 24 hours after a crisis is identified:
  - Arrange a meeting of and meet with the crisis management team;
  - Clearly establish the responsibilities of each member of the crisis management team;
  - If a member of the crisis management team or Board member, executive or other high level official in the organization is implicated in the crisis, consider creating a “wall” between the crisis management team and the individual(s) implicated;
  - Determine who must be notified (e.g., law enforcement, Board members or other management and governance bodies, employees, stockholders, outside counsel, public relations firms);
  - Begin to assess the Company’s disclosure obligations;
  - Determine whether a duty to preserve data has arisen and what steps must be taken to prevent spoliation;
  - Draft a response to potential media inquiries or initial public statements or press releases; and
  - Identify and cultivate key media contacts and prepare a social media strategy.

- When the duty arises, draft and circulate document preservation instructions to relevant personnel.
  - Document compliance with the preservation protocol; and
  - Collect relevant data and consider the scope of document review and production.

- As appropriate, conduct an internal investigation in response to the crisis:
Define the appropriate scope and scale of the investigation;

Establish appropriate processes to identify relevant data and witnesses and gather evidence, including through interviews of employees and third parties;

Consider whether separate legal representation of employees is warranted and, if so, identify competent outside counsel; and

Document findings and conclusions of investigation.

Identify relevant authorities, audiences and constituencies to whom disclosures and reporting will be made; carefully craft messages, emphasizing remedial measures.

Notify insurers and auditors as appropriate.

As necessary and appropriate, identify regulators and enforcement authorities and create a plan to cooperate and report to government entities.

Periodically test the Crisis Management Plan and the response of the Crisis Management Team.
B. Crisis Management Plans: Legal Considerations Checklist

- Identify competent outside counsel.
  - Identify counsel with expertise in the particular field or fields implicated in the crisis.

- Identify disclosure counsel and consider disclosure requirements.

- Consider attorney-client, work product and other legal privilege issues.

- Consider potential collateral consequences, including potential civil lawsuits.

- Consider special legal issues in foreign jurisdictions:
  - Consider legal obstacles to foreign document discovery (e.g., state secrecy, data protection laws, blocking statutes, legal privilege issues); and
  - Identify competent counsel in the relevant jurisdiction(s) (e.g., labor laws, other substantive legal issues).

- Preserve relevant documentation:
  - Determine when the duty arises and define scope;
  - Appoint an individual responsible for disseminating a preservation directive and documenting compliance;
  - Arrange for collection of potentially relevant data by competent service providers; and
  - Define the scope of document review.

- Conduct internal investigation, as appropriate.

- Report findings to insurers and auditors, as appropriate:
  - Understand Section 10A framework and notification requirements; and
  - Keep independent auditors apprised of developments.

- Report findings to government agencies:
  - Identify relevant government agencies;
  - Consider that settlement and charging documents will become publicly available; and
  - Emphasize remedial measures.
For issues involving data breaches or cybersecurity attacks, understand state and federal data breach notification requirements and engage competent counsel.

Consider employee issues:

- Consider need for separate legal representation and common interest privilege;
- Protect whistleblower rights;
- Consider appropriate disciplinary measure; and
- Liaise with HR and outside legal experts as necessary
XV. Endnotes


8 See Daniel E. Frank & Don Borelli, Hacked – Cybersecurity: How to Prepare for and Respond to Cyber Attacks, ASS’N OF CORP. COUNS. 40, 42, 44 (Mar. 2014); see also Stuart D. Levi et al., Skadden, Arps, Slate, Meagher & Flom LLP, Privacy and Data Security: Best Practices and Strategies for Success (Nov. 6, 2014).


11 See id. at 2-3.

12 See Section III.C for a discussion of the use of outside public relations specialists and certain special concerns associated with sharing sensitive information with these outside professionals.

13 See Daniel E. Frank & Don Borelli, Hacked – Cybersecurity: How to Prepare for and Respond to Cyber Attacks, supra note 8, at 38.

14 See id. at 38-39.
See Section III.A for a discussion of the spokesperson’s role in dealing with the media.


Pursuant to the U.S. Gramm-Leach Bliley Act, federally regulated financial institutions, upon discovering a security breach, must conduct an investigation to determine whether personal information was, or likely will be, misused and, if so, notify affected consumers. See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15, 736 (Mar. 29, 2005).


See generally Stuart Collins, Allianz Global Corp. & Specialty SE, A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity, supra note 16 (discussing the international regulatory landscape as it relates to cybersecurity).

See Section VIII for a more detailed discussion of assessing disclosure obligations in a crisis.


Alomari v. Ohio Dep’t of Pub. Safety, 626 F. App’x 558, 571 (6th Cir. 2015), cert. denied, 136 S. Ct. 1228 (2016) (“respond[ing] to . . . media inquiries [is] an act with great legal ramifications” and “[a]dvising a client on how to respond to media inquiries has important legal implications . . .”).


Id. at 54-55. With respect to work product protection, the court found that an otherwise valid assertion of work product protection is not waived “with respect to an attorney’s own work product simply because the attorney provides the work product to a public relations consultant whom he has hired and who maintains the attorney’s work product in confidence.” Id. The court noted, however, that “as a general matter public relations advice, even if it bears on anticipated litigation, falls outside the ambit of protection of the so-called ‘work product’ doctrine . . . .” Id.


Id.
Because *In re Grand Jury Subpoenas* involved an individual, the court’s opinion does not draw a distinction between outside counsel and in-house counsel. However, given the careful scrutiny with which courts are likely to analyze the relationship between a PR firm and the company, where outside counsel has been retained, it would be prudent for outside counsel to retain the PR firm. If outside counsel has not been retained, company counsel should follow these same guidelines and should be mindful that the court is likely to focus on the relationship between the PR firm and the company.

30 See Daniel E. Frank & Don Borelli, *Hacked – Cybersecurity: How to Prepare for and Respond to Cyber Attacks*, supra note 8, at 44.

31 See *id.*

32 Federal Rule of Civil Procedure 37(e) sets forth when and what sanctions federal courts may impose for the loss of electronically stored information (“ESI”). It does not apply to the loss of tangible items (e.g., hard copy documents). Fed. R. Civ. P. 37(e). Under this rule, sanctions are only available if ESI that “should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery.” *Id.* If a party suffers prejudice from the loss of ESI under these circumstances, a court “may order measures no greater than necessary to cure the prejudice.” *Id.* A court may only impose the most serious sanctions for the loss of ESI—an adverse inference instruction, dismissal of the action or a default judgment—“upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation.” *Id.*

33 Companies typically comply with their document preservation obligations by issuing a “document preservation directive” – also sometimes referred to as, among other things, a “litigation hold,” a “lit hold” or a “freeze directive” – which instructs company employees and representatives to preserve documents relevant to a particular subject matter or matters. The February 2008 ACC InfoPAK entitled *Implementing Legal Holds*, http://www.acc.com/legalresources/resource.cfm?show=19704, describes a process and technology-driven methodology and approach that a company can use when facing a legal hold.


six months before the plaintiff sent a legal hold notice because plaintiff’s CEO sent defendants text messages threatening to sue if they called his shareholders again even though he sent apologetic texts the next morning indicating he had been “upset” and drinking alcohol when he texted them the day before, and Zubulake, 220 F.R.D. at 217 (finding that defendant’s duty to preserve arose five months before the plaintiff filed an EEOC charge because emails of several employees indicated that such employees knew plaintiff intended to sue), with Scalera v. Electrograph Sys., Inc., 262 F.R.D. 162, 172 (E.D.N.Y. 2009) (finding that plaintiff’s filing of a worker’s compensation claim did not trigger a duty to preserve because the claim did not put defendants on notice that plaintiff would be filing a disability discrimination lawsuit against them), and Cache La Poudre Feeds, Inc. v. Land O’Lakes, Inc., 244 F.R.D. 614, 623 (D. Colo. 2007) (determining that demand letter regarding possible trademark infringement did not trigger a duty to preserve because the letter did not threaten litigation and addressed non-litigious resolution of the dispute).

36 See, e.g., Apple Inc. v. Samsung Elecs. Co., Ltd., 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012) (“[T]he duty to preserve extends to those employees likely to have relevant information—the ‘key players’ in the case.” (quoting Zubulake, 220 F.R.D. at 220)).

37 See, e.g., Pine Top Receivables of Ill., LLC v. Banco de Seguros del Estado, No. 12 C 6357, 2013 WL 3776971, at *2-3 (N.D. Ill. July 18, 2013) (finding that plaintiff had a duty to preserve relevant documents in the physical possession of a third-party because the plaintiff had a contractual right to access the documents); Haskins v. First Am. Title Ins. Co., Civil No. 10 - 5044 (RMB/JS), 2012 WL 5183908, at *4-5 (D.N.J. Oct. 18, 2012) (same); GenOn Mid-Atl. LLC v. Stone & Webster, Inc., 282 F.R.D. 346, 353-55 (S.D.N.Y. 2012) (finding that plaintiff had a duty to preserve relevant documents in the physical possession of its litigation consultant because it had the practical ability to obtain the documents on demand), aff’d, No. 11 CV 1299(HB), 2012 WL 1849101 (S.D.N.Y. May 21, 2012).

38 See, e.g., Selectica, Inc. v. Novatus, Inc., No: 6:13-CV-1708-ORL-40, 2015 WL 1125051, at *4 (M.D. Fla. Mar. 12, 2015) (“‘Control’ has been construed broadly by the courts as the legal right, authority, or practical ability to obtain the materials sought upon demand.” (citation omitted)); Pine Top Receivables of Ill., 2013 WL 3776971, at *2 (“On the issue of control, it is well-settled that a party need not have actual possession of the documents to be deemed in control of them. Instead, the test is whether the party has a legal right to obtain them.” (internal quotation marks omitted) (citation omitted)).

39 See, e.g., Selectica, Inc., 2015 WL 1125051, at *4 (finding that the defendant had a duty to preserve relevant files on the personal cloud-based data storage account of its employee because it had the practical ability to access the files saved in the storage account); In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig., MDL No. 2385, 2013 WL 6486921, at *18 (S.D. Ill. Dec. 9, 2013) (finding that the defendant’s preservation directive applied to relevant business-related texts messages on its employees’ personal cell phones), order rescinded in part on other grounds by 745 F.3d 216 (7th Cir. 2014).

40 See Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC, No. 08-0840-CV-W-ODS, 2012 WL 3047164, at *3-6 (W.D. Mo. 2012) (ordering sanctions for spoliation, in part, due to defendant’s failure to preserve the ESI of a departing employee).
In today’s world, the focus has shifted from paper documents (though they still remain relevant and must be preserved) to information stored electronically. ESI includes any information stored in an electronic format and includes, but is not limited to, emails, voicemails, instant messages, text messages, presentation files, spreadsheets, word processing files, databases, file fragments, metadata, picture files, social media accounts, web-based applications, and web pages. The Federal Rules of Civil Procedure expressly address ESI. See, e.g., Fed. R. Civ. P. 16, 26, 33, 34, 37, 45. The recent 2015 amendments to the Federal Rules of Civil Procedure added new provisions regarding the preservation of ESI by (1) creating a uniform standard for sanctions for the loss of ESI, Fed. R. Civ. P. 37(e); (2) requiring that the parties’ discovery plan state their views and proposals on any issues about preservation of ESI, Fed. R. Civ. P. 26(f)(3)(C); and (3) providing that a court’s case scheduling order may require preservation of ESI, Fed. R. Civ. P. 16(b)(3).

See, e.g., Apple Inc. v. Samsung Elecs. Co., Ltd., 888 F. Supp. 2d 976, 991 (N.D. Cal. 2012) (finding that once the defendant’s duty to preserve took effect it was “required to suspend any existing policies related to deleting or destroying files and preserve all relevant documents related to the litigation” (quoting In re Napster, Inc. Copyright Litig., 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006)); Phillips Elecs. N. Am. Corp. v. BC Tech., 773 F. Supp. 2d 1149 (D. Utah 2011) (“Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”) (quoting Zubulake, 220 F.R.D. at 218)). Depending on the nature of the crisis and the company’s electronic systems and back-up policies, it may be prudent to pull and preserve the set of back-up tapes made immediately prior to the crisis.


See Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (“The litigation hold instructions must be reiterated regularly and compliance must be monitored.”).

Companies should consider retaining a third-party vendor to harvest ESI. Such vendors follow established and defensible procedures designed to harvest ESI without altering the ESI or its metadata and can provide independent testimony in the event the harvesting process is challenged. In certain circumstances, however, it may be necessary for the company’s IT staff to harvest ESI, such as when the company’s security policies prohibit third parties from accessing their ESI systems or when timing or logistical issues preclude using third-party vendors. If the company’s IT staff is going to harvest ESI, it too must take steps to ensure that the ESI and its metadata are not altered as a number of courts have held that such altered metadata constitutes spoliation and have sanctioned parties that have produced ESI with altered metadata. See, e.g., T&E Inv. Grp., LLC v. Faulkner, Nos. 3:11-CV-0724-P, 3:11-CV-1558-P, 2014 WL 550996, at *5-6 (N.D. Tex. Feb. 12, 2014) (giving an adverse inference instruction to the jury and ordering monetary sanctions for defendant’s intentional alteration of metadata).

Documenting the chain of custody for ESI should follow strict protocols to maintain the strongest levels of defensibility in the event that spoliation claims are made in connection with the information that is produced and ultimately sought to be introduced into evidence. Documenting the chain of custody generally should not fall to the company’s attorneys.
because conflicts may arise if they are called upon to testify as fact witnesses regarding how the data was collected.


50 See id. at art. 2(a).

51 See id. at art. 2(b).

52 See generally id. at Chapter IV.

53 See, e.g., Norbert Nolte & Christoph Werkmeister, Data Protection in Germany: Overview, PRACTICAL L., http://us.practicallaw.com/3-502-4080#a514865 (noting that Germany’s Federal Data Protection Act (BDSG) provides special rules for certain types of data (for example, information on a person’s racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, or sex life); Roland Mathys, Data Protection in Switzerland: Overview, PRACTICAL L., http://uk.practicallaw.com/9-502-5369#a465597 (noting that special rules apply for sensitive data like religious, ideological, and political views and activities; health, the intimate sphere or racial origin; social security measures; and administrative or criminal proceedings and sanctions).

54 For a list of countries that the European Commission has found do offer an “adequate level of protection,” see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm Please note that although some aspects of U.S. law have been deemed to be in compliance, the European Commission has not made a general finding with respect to the entire nation as it has for other countries.


58 Id. (emphasis omitted).

59 Id.


61 See id.

62 See id.


66 See supra note 64, at 2.

67 “An adequacy decision is an acknowledgement that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments. Such adequacy decisions will be taken at European level on the basis of explicit criteria which will also apply to police cooperation and criminal justice.” EUROPEAN COMMISSION, *How Will the EU’s Data Protection Reform Make International Cooperation Easier?*, (emphasis omitted), http://ec.europa.eu/justice/data-protection/files/5_reform_en.pdf.

68 Id.


74 French Penal Code Law No. 80-538, art. 1A (July 16, 1980).


77 Available at https://www.justice.gov/opa/file/838386/download.

78 Id. at 2.

79 Id. at 6.

80 Id.


In light of the recent “Yates Memorandum,” which sets forth the Department of Justice’s policy of seeking to hold individuals accountable for corporate misconduct, a company must understand the range and scope of its D&O insurance policies. In particular, counsel should familiarize themselves with provisions related to the advancement of legal fees for directors and officers facing enforcement actions, including “final adjudication” language which dictates the point at which an insurer can withhold defense costs and whether the policies cover investigative costs if a suit is not filed. Companies that do not currently have D&O insurance policies may wish to consider adding such coverage. See generally Memorandum from Sally Quinn Yates, Deputy Attorney General, on Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), https://www.justice.gov/dag/file/769036/download.

The SEC launched “Operation Broken Gate” in October 2013 to hold accountable auditors who have intentionally or negligently violated professional auditing or accounting standards. Since then, the SEC has increasingly prioritized enforcement actions against auditors, especially under SEC Rule of Practice 102(e), which was codified in the Sarbanes-Oxley Act and allows the SEC to seek sanctions against accountants. The SEC charged 21 individuals under Rule 102(e) in the first five months of 2016 alone. See, e.g., In the Matter of Malonebailey, LLP, and Jay Phillip Norris, CPA, Exchange Act Release No. 77755 (May 2, 2016); In the Matter of Monsanto Company, Sara M. Brunquell, CPA, Anthony P. Hartke, CPA, and Jonathan W. Nienas, Securities Act Release No. 10037, Exchange Act Release No. 77087 (Feb. 9, 2016).

Audits of this nature would likely evaluate the following: (1) where is the data coming into the company?; (2) how is data used and what controls are in place?; (3) how are security decisions made and implemented?; (4) do internal and external privacy policies align with actual practice?; (5) what is the company saying about its security policies?; (6) what is the company disclosing in its public filings?; (7) how are company executives and board members kept informed?; (8) how mature is the privacy program?; (9) what sort of training/retraining is provided?. See Stuart D. Levi, et al., Skadden, Arps, Slate Meagher & Flom LLP, Privacy and Data Security: Best Practices and Strategies for Success (Nov. 6, 2014).


The SEC interprets Section 10A to apply to illegal acts beyond financial misconduct and even beyond an employee’s business responsibilities. Specifically, Staff Accounting Bulletin 99 notes that – in contrast to audit literature – the definition of “illegal act” in Section 10A...


99 Compare Medinol, Ltd. v. Boston Scientific Corp., 214 F.R.D. 113, 115-17 (S.D.N.Y. 2002) (holding that disclosure of attorney work product to an auditor waives the protection), with Merrill Lynch & Co. v. Allegheny Energy, Inc., 229 F.R.D. 441, 446-47 (S.D.N.Y. 2004) (holding that disclosure of attorney work product to an auditor does not waive the protection because an independent auditor is not an adversary within the meaning of the attorney work product doctrine). See also S.E.C. v. Berry, No. C07-04431 RMW (HRL), 2011 WL 825742, at *7 (N.D. Cal. Mar. 7, 2011) (stating that the court in Merrill Lynch correctly concluded that disclosure to an outside auditor does not represent the type of adversarial relationship necessary to constitute waiver of the attorney work product protection); Westernbank P.R., 2009 WL 530131, at *4-8 (holding that disclosure of attorney work product to an auditor does not waive the protection and noting that Medinol has been “roundly criticized”). Cf. United States v. Baker, No. A-13-CR-346-SS, 2014 WL 722097, at *2 (W.D. Tex. Feb. 21, 2014) (explaining that voluntary disclosure to an outside auditor does not necessarily waive the attorney work product protection because such disclosure does not always undercut the adversary process) (citing Deloitte, 610 F.3d at 140)).


103 A new section addressing civil liability for individuals was also added. See USAM § 4-3.100. The U.S. Attorney’s Manual is available at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/.


106 Yates Memorandum, supra note 87.


109 Id.

110 Id.

111 USAM § 9-28.720.


114 Andrew Ceresney, Director, Division of Enforcement, Securities and Exchange Commission, Remarks at University of Texas School of Law’s Government Enforcement


Andrew Ceresney Remarks, supra note 114.

SEC Press Release, supra note 115 (identifying the following four considerations: “[t]he assistance provided by the cooperating individual,” “[t]he importance of the underlying matter in which the individual cooperated,” “[t]he societal interest in ensuring the individual is held accountable for his or her misconduct,” and “[t]he appropriateness of cooperation credit based upon the risk profile of the cooperating individual.”).


For a detailed discussion of the potential for privilege waiver and practical steps to avoid such waiver in the context of disclosures to the government and in other parallel proceedings, see Section X.

To minimize the potential for later disputes regarding oral reports, a company and its counsel should maintain detailed memos of discussions with regulators and investigators.


U.S. Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, supra note 19 (“Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents.”).

See 17 C.F.R pt. 229.

(“An investigation on its own is not a ‘pending legal proceeding’ until it reaches a stage when the agency or prosecutorial authority makes known that it is contemplating filing suit or bringing charges.”) (quoting David M. Stuart & David A. Wilson, Disclosure Obligations Under the Federal Securities Laws in Government Investigations, 64 BUS. LAW. 973, 982 (2009)).


127 See id.


129 See Winer Family Tr. v. Queen, 503 F.3d 319, 329 (3d Cir. 2007) (stating that an affirmative duty to disclose may arise when there is “an inaccurate, incomplete, or misleading prior disclosure”); see also Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund, 135 S. Ct. 1318 (2015) (emphasizing the obligation not to mislead through omissions under the Securities Act even when the affirmative statements made were accurate).


132 “Upjohn warnings” are named after the Supreme Court case of Upjohn Co. v. United States, 449 U.S. 383 (1981). Typically, Upjohn warnings include statements that (1) the interview is being conducted by an attorney who represents the company; (2) the attorney does not represent the witness; (3) the purpose of the interview is to obtain information in order to provide legal advice to the company and, therefore, the interview discussion will be subject to privilege; (4) the privilege belongs to the company and not the witness; (5) the witness should not discuss the contents of the interview unless authorized; and (6) the company, in its sole discretion, may decide to waive the privilege and disclose the contents of the interview to any third party.

133 See Section VII.B. The Yates Memo outlines “six key steps” guiding and strengthening the DOJ’s actions in “pursuit of individual corporate wrongdoing,” which include: “(1) in order to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct; (2) criminal and civil corporate investigations should focus on individuals from the inception of the investigation; (3) criminal and civil attorneys handling corporate investigations should be in routine communication with one another; (4) absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation; (5) Department attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases, and should memorialize any declinations as to individuals in such cases; and (6) civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual’s ability to pay.” Yates Memorandum at 2-3.

134 See USAM § 9-28.720.

572 F.2d 596, 611 (8th Cir. 1978) (en banc).

*See In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127 (9th Cir. 2012) (discussing cases); *In re Quest Commc’ns Int’l Inc.*, 450 F.3d 1179, 1187–88 (10th Cir. 2006) (same); *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 295–302 (6th Cir. 2002) (same); *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1425 (3d Cir. 1991) (”[S]elective waiver does not serve the purpose of encouraging full disclosure to one’s attorney in order to obtain informed legal assistance; it merely encourages voluntary disclosure to government agencies, thereby extending the privilege beyond its intended purpose.”).

9 F.3d 230, 236 (2d Cir. 1993); *see also In re Quest Commc’ns Int’l, Inc.*, 450 F.3d at 1182, 1194; *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1127 (7th Cir. 1997); *United States v. Billmyer*, 57 F.3d 31, 37 (1st Cir. 1995).


679 F.3d at 1128-29.

*See S.E.C. v. Berry*, No. C07-04431 (RMW) (HRL), 2011 WL 825742, at *4 (N.D. Cal. Mar. 7, 2011) (analyzing whether “confidentiality agreements” with the SEC and other government entities waived work product protections without any mention of FRE 502 or section (e) of the Rule). But see *Pac. Pictures Corp.*, 679 F.3d at 1129 (citing the legislative history of FRE 502, which was intended to clarify privilege and waiver for parties facing large document productions, and concluding that nothing in the rule suggested that encouraging government cooperation was sufficient reason to apply a “limited form of selective waiver”).

A court must still find a source of procedural authority to issue the order, such as Federal Rules of Civil Procedure 26 or 16.


*Spieker v. Quest Cherokee, LLC*, No. 07-1225-EFM, 2009 WL 2168892, at *3 (D. Kan. July 21, 2009) (holding that “[s]imply turning over all ESI materials does not show that a party has taken “the reasonable steps” to prevent disclosure of its privileged materials”); *United States v. Sensient Colors, Inc.*, Civ. No. 07-1275 (JHR/JS), 2009 WL 2905474, at *3 (D.N.J. Sept. 9, 2009) (applying the elements of FRE 502(b), including “reasonable steps”).
145 See Fed. R. Evid. 502 advisory committee’s note (“For example, the court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of ‘claw-back’ and ‘quick peek’ arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product.”).

146 FRE 502(b) provides that a disclosure in a federal proceeding or to a federal office or agency does not operate as a waiver if a three-step test is met. The disclosure must be inadvertent, the holder of the privilege or protection must have taken reasonable steps to prevent disclosure and the holder must have promptly taken reasonable steps to rectify the error, including, if applicable, following Federal Rule of Civil Procedure 26(b)(5)(B). Again, courts have diverged on the meaning of this provision, especially regarding whether inadvertent simply means “the production [of the document] was a mistake.” See Coburn Grp., LLC v. Whitecap Advisors LLC, 640 F. Supp. 2d 1032, 1038 (N.D. Ill. 2009) (discussing cases).

147 Compare Columbia/HCA Healthcare, 293 F.3d at 306-07 (agreement has no effect) with Steinhardt, 9 F.3d at 236 (an “explicit agreement” may change the outcome) and Permian Corp. v. United States, 665 F.2d 1214, 1215 (D.C. Cir. 1981) (agreement preserved work product protection but not attorney-client privilege).

148 Compare In re Martin Marietta Corp., 856 F.2d 619, 626 (4th Cir. 1988) (protecting opinion work product from disclosure, despite waiver of protection over all fact work product relating to the same subject matter) with Westinghouse Elec. Corp., 951 F.2d at 1431 n.17 (indicating that the distinction between fact and opinion work product may be irrelevant to the waiver analysis).

149 See note 151 infra.

150 See Martin Marietta, 856 F.2d at 623, 625; In re Sealed Case, 676 F.2d 793, 824 (D.C. Cir. 1982); In re Leslie Fay, 161 F.R.D. at 282-84.


153 Id.

154 Id. at 373.

155 Ryan v. Gifford (Ryan I), No. 2213-CC, 2007 WL 4259557 (Del. Ch. Nov. 30, 2007) (letter opinion). The court indicated in a subsequent opinion denying certification for interlocutory appeal that the company also had provided certain related documents to the SEC and the United States Attorney’s Office, and had disclosed a copy of the completed

156 See Ryan I, 2007 WL 4259557, at *3. In an alternative holding, the court found that plaintiffs established “good cause” for disclosure under the rule of Garner v. Wolfinbarger, 430 F.2d 1093, 1103-04 (5th Cir. 1970), available to stockholders in suits against company fiduciaries. See Ryan I, 2007 WL 429557, at *3.

157 See Schaeffler v. United States, 806 F.3d 34, 40 (2d Cir. 2015); see also In re Santa Fe Int’l Corp., 272 F.3d 705, 711 (5th Cir. 2001) (“[T]here must be a palpable threat of litigation at the time of the communication . . . before communications between one possible future co-defendant and another . . . could qualify for protection.”).

158 See, e.g., Walsh v. Northrop Grumman Corp., 165 F.R.D. 16, 18 (E.D.N.Y. 1996) (“The doctrine does not extend to communications about a joint business strategy that happens to include a concern about litigation.”); Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A., 160 F.R.D. 437, 447 (S.D.N.Y. 1995) (“The common interest doctrine does not encompass a joint business strategy which happens to include as one of its elements a concern about litigation.”).

159 See, e.g., Schaeffler, 806 F.3d at 40–42.

160 United States v. Gonzalez, 669 F.3d 974 (9th Cir. 2012) (finding that a common interest may be created or terminated thought conduct as well as through an express agreement).


164 In re Grand Jury Subpoena: Under Seal, 415 F.3d 333, 341 (4th Cir. 2005) (declining to extend the privilege to communications shared during fact-gathering interview prior to the existence of an agreement, where the purpose of such interview was to assess whether the parties shared a common interest in the first place); see also Hunton & Williams v. U.S. Dep’t of Justice, 590 F.3d 272, 286 (4th Cir. 2010) (explaining that just because two parties later “concluded [they] shared [a common] interest does not protect communications between the two before that decision was made.”).

165 430 F.2d at 1103–04 (providing factors for disclosure of privileged company materials to shareholders in a derivative action).

166 In re Perrigo Co., 128 F.3d 430, 440–41 (6th Cir. 1997).

167 Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 125 (2d Cir. 2006) (remanding for a factual determination of whether “defendants waived the privilege by placing in issue the contents of the privileged information”).
Crisis Management: in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in a Global Environment

168 *In re Chrysler Motors Corp. Overnight Evaluation Program Litig.*, 860 F.2d 844, 846 (8th Cir. 1988).

169 *Three Rivers Dist. Counsel v. Governor & Co. of the Bank of Eng.* (No.6), [2004] UKHL 48, (finding that the legal advice privilege extends to advice on how the client should present its evidence, rather than being limited to advice concerning legal rights and obligations).


173 See supra notes 84 and 132.


175 See id. at 340-41.


177 The company also should consider identifying key individuals at the onset of a crisis and attempting to secure their cooperation should their employment terminate before crisis-related proceedings conclude. This can be accomplished through an appropriately drafted severance or exit agreement, which may require the individual to be available for consultation on the matter or to maintain company confidences. To the extent the agreement contains confidentiality or non-disparagement clauses, it may be appropriate to also include a provision that makes clear that the agreement would not prohibit the individual from making communications to a court or administrative agency. Moreover, if the company is cooperating with governmental authorities, it may be appropriate to include an express cooperation clause that requires the individual to cooperate with a governmental investigation, including making himself or herself available for testimony.

178 Another way to reduce fees in such circumstances is through the establishment of a shared document repository. Careful consideration should be given to the manner in which such a repository is established, including, for example, whether to limit certain individuals’ access to documents maintained in the repository or to omit from the repository privileged communications.

179 17 C.F.R. § 203.7(b).

180 See *SEC v. Csapo*, 533 F.2d 7, 11 (D.C. Cir. 1976) (finding the sequestration rule to be inconsistent with the right to choice of counsel under the Administrative Procedure Act (“APA”), and requiring the SEC to provide “‘concrete evidence’” that an attorney’s presence would “obstruct and impede its investigation” before excluding the attorney); *SEC v. Higashi*, 359 F.2d 550 (9th Cir. 1966) (holding that the sequestration rule as applied prejudiced the witness’s interests, in violation of the APA).
See, e.g., Cal. Labor Code § 2802(a) (2016) ("An employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer, even though unlawful, unless the employee, at the time of obeying the directions, believed them to be unlawful.").


USAM § 9-28.730.

Id.

541 F.3d 130 (2d Cir. 2008).

Revisions to the USAM further provide that the “mere participation by a corporation in a joint defense agreement does not render the corporation ineligible to receive cooperation credit, and prosecutors may not request that a corporation refrain from entering into such agreements.” USAM § 9-28.730.

Yates Memorandum at 4, supra note 87.

Seaboard Report, supra note 113.

See id.

McNulty Memorandum at 11, supra note 184.

Filip Letter at 3 (emphasis omitted), supra note 185.

USAM § 9-28.1000.

Id. at § 9-28.800.


Apart from DOJ and SEC, state regulators may also look to and require discipline of culpable individuals when entering settlements. For example, as part of the New York Department of Financial Services’ (“DFS”) 2015 settlement with Deutsche Bank regarding its LIBOR-related conduct, DFS “order[ed] the Bank to take all steps necessary to terminate seven employees [in the Bank’s London and Frankfurt offices], who played a role in the misconduct but who remain employed by the Bank.” NYDFS Announces Deutsche Bank to Pay $2.5 Billion, Terminate and Ban Individual Employees, Install Independent Monitor for Interest Rate Manipulation, DFS Press Release (Apr. 23, 2015), http://www.dfs.ny.gov/about/press/pr1504231.htm.

See, e.g., Egan v. TradingScreen, Inc., No. 10 Civ. 8202(LBS), 2011 WL 1672066 (S.D.N.Y. May 4, 2011) (holding that, under certain circumstances, the anti-whistleblower retaliation provisions of the Dodd-Frank Act may protect an employee who provides information to the outside counsel conducting the internal investigation if the outside counsel later reports the information to the SEC).


210 See id. (discussing the SEC’s extension of the protective status of “whistleblower” to any person who, acting alone or jointly, provides information to the SEC about a potential securities law violation).

211 See, e.g., United States ex rel. Wildhirt v. AARS Forever, Inc., No. 09 C 1215, 2013 WL 5304092 (N.D. Ill. Sept. 19, 2013) (collecting cases, allowing defendant’s counterclaims for breach of contract and indemnification pursuant to a confidentiality provision in relator’s employment agreement to proceed in case relators failed to succeed on the merits)


214 In the Matter of KBR, Inc.