CORPORATE INTERNAL INVESTIGATIONS

The information contained in these MCLE materials should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of ACC or of Wilson Sonsini Goodrich & Rosati or any of its lawyers, unless so stated. The information contained in these materials is not intend to be a definitive statement on the subject but rather to serve as a resource providing practical information for the reader.

ACC wishes to extend a special thanks to the following individuals for their assistance with updates to these materials:

Fred W. Alvarez, Partner, Wilson Sonsini Goodrich & Rosati

&

Leo Cunningham, Partner, Wilson Sonsini Goodrich & Rosati

For more information about the contributors go to:

http://www.wsgr.com

DISCUSSION

Issues

1. When confronted with possible wrongdoing within the company, when should a company immediately notify the government or first conduct an investigation and then notify the government?

2. If a company notifies the government immediately upon learning about possible wrongdoing, how should it respond if the government asks it to withdraw from the market a product whose safety or effectiveness may be questionable if such wrongdoing occurred?

3. If a company decides to conduct an internal investigation of alleged wrongdoing before contacting the government:

a). When should it use outside counsel (or other consultants/contractors) and when should it conduct the investigation with inside counsel?

b). When should the company conduct an informal preliminary inquiry limited to certain persons before launching a full-fledged investigation?

c). When should the Board be notified and what role should it play? Who should talk to the board and how should that conversation be noticed?

d) Should Chris, who worked on the Nolip project, be included on the team investigating the matter?

e) Should the Chief Compliance Officer be included on a company team investigating possible wrongdoing by employees?

f) Should the investigative report be written or oral? What should it contain? What is "fact" and what is potentially attorney work product protected?

4. If a company receives an allegation against employees whose legal expenses it normally would cover, should it indicate to the government at the outset of an investigation that it will not pay those expenses in order to emphasize the company's willingness to cooperate?

5. Can a company tell employees that it will fire them if they don't cooperate with a company investigation that is conducted at the behest of the government, or whose results will be shared with the government?

6. When a company is preparing to conduct a confidential investigation of alleged wrongdoing, what public comments can an officer make if faced with questions that relate in some way to the subject matter of the investigation?

Discussion

1. When confronted with possible wrongdoing within the company, when should a company immediately notify the government or first conduct an investigation and then notify the government?

If the company is especially concerned about the prospect of criminal prosecution, it may want to not only be in touch at some point with the relevant regulator (in this scenario, the FDA, but in other instances it could be the SEC or another agency), but should consider the Department of Justice (DOJ) guidelines on Federal Prosecution of Business Organizations (set forth in the U.S. Attorney's Manual §§ 9-28.000 to 9-28.1300, the current version of which is known as the "Filip Memo"). Section 9-28.700 of those guidelines says that a company's "timely and voluntary disclosure of wrongdoing and its cooperation with the government's investigation may be relevant factors" in determining whether to bring criminal charges against a corporation. In evaluating the extent of cooperation, a prosecutor may consider the company's "willingness to provide relevant evidence and to identify the culprits within the corporation."

On one hand, immediately going to the government establishes especially timely disclosure by the corporation, which could be helpful in influencing the exercise of prosecutorial discretion in the company's favor. And when the possible crime is an antitrust violation, the company may want to try to take advantage of a formal leniency program that provides amnesty for the first conspirator to report an antitrust conspiracy. In addition, the company would strongly prefer that the government learn of any wrongful conduct from the company. The longer it waits, the greater the risk that a panicky employee will inform the government in the hope of gaining lenient treatment (or a whistleblower reward) or that someone will leak something to the media. Such an employee could well claim that high company officials gave the order to falsify the data. Even if eventually proven false, this claim could create a presumption against the company at the start that the company will spend all of its time trying to counter, rather than telling the story of what they're doing as part of the pool of those victimized by this horrible crime. Once perceptions are set, they are hard to dispel.

On the other hand, informing the government before conducting any investigation means there will be no avoiding the costs of dealing with the government—even if it turns out there is no reason for it. Premature contact with the government also increases the likelihood of the government taking actions such as conducting its own investigation severely limiting the discretion the company would otherwise have to make its own judgment about the conduct that occurred and how it should respond to it. It places the company in the position of having to justify those decisions, no matter how the investigation comes out. At this point, the company has received an allegation from one employee. Officials have not confirmed his story with anyone else, and it is at least possible that he may be exaggerating for any number of

reasons. Further investigation could indicate that there has been a misunderstanding on Jim's part, that perhaps he bears a grudge against other team members, that there have been only minor transgressions that create no health hazard, or that no one followed Karl's instructions to falsify the data. Rather than place the company immediately in a poor light with the government and do irreparable and irreversible harm, it may be preferable first to gather more information to determine more precisely what happened.

The judgment call for the company here is not an easy one: does the flexibility inherent in not immediately reporting to the government justify the risk that an "unsupervised" investigation will be perceived as not a serious one? If the company decides to proceed internally first, it should be asking itself, at every step, "how will this look down the road?"

2. If a company notifies the government immediately upon learning about possible wrongdoing, how should it respond if requested to withdraw from the market a product whose safety or effectiveness may have been affected if such wrongdoing occurred?

Corporate counsel might suggest that doing so would be premature at this point because there's no evidence that Nolip was implicated in the woman's death, nor has anyone verified Jim's allegations. What if the corporation withdraws the drug, and Jim's allegations turn out to be unfounded? Withdrawal could cause an unnecessary panic among patients, while depriving them of a drug that could be both effective and safe. The corporation's stock price may plummet, employees may leave the company; suppliers and other partners may distance themselves from a company whose reputation is tarnished. Funding could dry up and government contracts could be suspended. Furthermore, notwithstanding exoneration, Wilshire's reputation may likely would be tarnished, as would the public's confidence in Nolip.

On the other hand, depending on the facts, some people could be in danger, and immediate withdrawal would eliminate the risk that they may be facing, as well as minimizing damages that the company may incur. Immediate withdrawal also could allow the company to gain favor by setting a "responsible" tone for the government, as well as with the larger public. If the company refuses to withdraw now, and the investigation later verifies Jim's allegations, the company could be subject to intense criticism for protecting its interests over those of patients.

Withdrawing the drug now is likely to win the company more points with the government than with the public. Johnson & Johnson, for instance, received praise when it voluntarily withdrew Tylenol from the market after third-party tampering with the drug resulted in deaths. Johnson & Johnson, however, largely was seen as an innocent victim of wrongdoing. By contrast, if anyone is in danger in this case, it may be because Wilshire engaged in wrongdoing. Voluntary withdrawal of the drug under these circumstances may well gain the company little approbation from the public and could confirm their suspicions that the company is guilty of something before the facts are even in.

The corporation's decision and counsel's recommendation may rest upon how likely counsel believes Jim is telling the truth. The higher the probability that he is, the greater the risk to the public and the company from not withdrawing Nolip now. No matter what the

decision the company should investigate the Nolip development and application process and determine exactly what happened.

3. If a company decides to conduct an internal investigation of alleged wrongdoing before contacting the government:

a) When should it use outside counsel (or other consultants/contractors) and when should it conduct the investigation with inside counsel?

Using in-house counsel may be preferable if the allegations relate to relatively simple wrongdoing by low-level employees. In those cases, in-house counsel can offer efficiencies in terms of the lower cost and greater speed with which a lawyer familiar with the company's business and procedures may be able to conduct the investigation. The key consideration should be, "how will this look?" especially if the conclusion turns out to be that no wrongdoing occurred. It is also critical to remember that while internal investigations – whether done by inside or outside counsel – will all start out as privileged ones, practical realities may lead to a need to waive the privilege at some point in the future when the company decides it needs to show that it took the matter seriously, and "did the right thing." In that sense, the question of who does the investigation is really a question of "who do we want to testify about what we did and why?"

In this case, the CEO prefers not to bring in outside counsel at this point because he is concerned that information may be disclosed outside the company. That should not be a risk, however, with the use of responsible and experienced outside counsel, who obviously will have confidentiality obligations to the company. It is true, however, that the more people who are involved, the more likely that someone (or someone they work with or live with) could repeat information. What the CEO seems to suggest here is a fundamental concern that many leaders in companies have when allegations like these surface: a fear that they won't be able to control the flow of information and the almost primal tendency to hope that if no one finds out about it, perhaps it never happened. Obviously, part of the lawyers' job in this situation is to help the CEO overcome his urge to go to ground and to develop a strategy that allows him the comfort of knowing that corporate counsel is doing their best to manage the situation, even as counsel can't control the outcome.

In this instance it may be wise to use outside counsel. First, the allegation that Karl, the head of Product Development, instructed employees to falsify data means that a relatively high-ranking company official could be involved in wrongdoing. The government may be especially concerned that the company will have a motive to minimize the scope of the misconduct to lessen the likelihood of any action against the corporate entity. Using outside counsel may ease this concern, because it may signal that the company is willing to have an independent investigator look at the facts and let the chips fall where they may.

Second, the alleged misconduct is extremely serious because of its possible impact on health and safety. For a pharmaceutical company, even a hint of dishonesty in submitting

scientific data could be fatal to its credibility with the public and with regulators. Hiring outside counsel may serve to underscore to outsiders that the investigation will be conducted by an independent party who has no motive to overlook or minimize any wrongdoing. In order to accomplish this goal, the company may not want to hire outside counsel who has done extensive work for it. This will lead people to question whether the firm is any more independent in its assessment than in-house leaders would be. Selection of outside counsel may – like it or not – influence the government's assessment of the extent of the company's cooperation. If avoiding criminal charges is a paramount consideration, the company may want to exercise every opportunity to signal its cooperativeness and its willingness to be completely forthcoming.

When the allegation involves remote locations, sensitive personal issues, or technical or forensic expertise that investigators have but lawyers don't, it may be worth thinking beyond the outside counsel box. There are other contractors that could be considered, including private investigators and corporate internal investigation specialists, who could be asked to dig up additional information, review documents, or conduct interviews in support of an in-house or outside counsel-led investigation team.

While these kinds of consultants serve important roles in some kinds of investigations, they can also bring problems in others. They may not be sensitive to how their tactics will look when judged by regulators or the public. Consider, for instance, the Hewlett-Packard investigators who engaged in "pretexting" in order to glean information about board members' communications in an effort to uncover the source of alleged leaks of board level information. The lesson is to use contractors carefully, supervise them carefully, and use only those contractors that will enhance the company's credibility.

b) When should the company conduct an informal preliminary inquiry limited to certain persons before launching a full-fledged investigation?

This decision depends on how serious and credible the allegation of wrongdoing is, and on how urgently a full investigation needs to be conducted. Generally, the more serious and credible the allegation, the greater the company's interest in determining as soon as possible what has occurred. In this case, Jim has claimed that a high-level official instructed employees to commit fraudulent acts that may have endangered members of the public. While it's not clear that the company's drug was implicated, one person taking it has already died from the type of side effects that Jim maintains the company concealed in its application for regulatory approval. Finally, the damage to the company from disclosure of these allegations before the company has had an opportunity to investigate them could be devastating. For these reasons, time is of the essence, and the company may want to initiate a full investigation as soon as possible.

c) When should the Board be notified, what role should it play, and who should notify it?

The impact of the alleged wrongdoing on the company and/or the level of employees involved should be the main considerations in determining whether to notify the board upon

receiving an allegation. In this case, if employees falsified data on the side effects of Nolip in order to obtain FDA approval, the company could be subject to criminal prosecution. However substantial the financial impact of prosecution, the reputational harm to the company likely would be even greater. Similarly, if key executives are implicated, the Board will need some visibility into the process to ensure that facts are objectively considered. Loss of public confidence in the integrity of the company and its executives, and the safety of its products could seriously impair its ability to do business and could lead to its demise. Depending on how events unfold, the company could have no choice but to enter into a deferred prosecution agreement with the government. This would subject the corporation to oversight by a monitor, with any breach of the monitorship agreement serving as the possible basis for immediate indictment.

In light of these risks, the Board should be apprised of the allegations and should be kept informed of the progress of the investigation. While there likely will be no need for the Board to make decisions about the details of this investigation, directors will need to be prepared to make important decisions once it ends and to be informed and engaged in directing the big decisions that will flow. These include matters such as when and how to notify the government, whether the company will be paying attorneys' fees for persons suspected of wrongdoing, what disciplinary action to take against culpable officers or employees, whether privilege will be waived to the government or others, and what steps it is willing to take to assist the government in the prosecution of any individuals.

In this scenario, Max as the CCO reports directly to the audit committee, presumably with this kind of report contemplated as exactly the kind of report he should make. His decisions are not so much whether to report, but when and how serious he should make this for them: a notice that there's an investigation, or a detailed report that the sky could be falling? While Ted, the CEO is clearly also welcome to deliver this news personally to the audit committee or board leadership, Max should be concerned if he's been asked to delegate that role to the CEO, especially if it might be hard for him to later verify what was said, or perhaps more poignantly, what was not said. Max may be hired, evaluated, and even fired by the CEO, but he reports to the board; in that role, he is somewhat akin to the CLO in terms of fiduciary responsibility and "client" relationship.

d) Should Chris, who worked on the Nolip project, be included on the team investigating the matter?

No. There may be no indication of any fault with the attorney's work on that project. There is at least the potential, however, that her investigative work could be colored by a desire to avoid being regarded as negligent or even reckless in failing to detect the falsification. This creates the prospect that she will have a conflict of interest under Model Rule 1.7(a)(2), because there could be a significant risk that her representation of the company in the investigation "will be materially limited by" her personal interest.

In addition, if the situation unfolds that the company is involved in legal proceedings as a result of the investigation, the attorney could be called as a witness to testify about the activities of the Nolip project team. Under Model Rule 3.7, the attorney could not represent

the company in that proceeding despite having participated in the investigation. It would be advisable to create an investigative team whose members would not be hobbled by this limitation.

e) Should the Chief Compliance Officer or someone from that office be included on a company team investigating possible wrongdoing by employees?

In this company, the CCO is not part of the general counsel's office and reports directly to top management. Max's job is to help design the compliance program, educate employees about it and encourage them to come forward with reports of misconduct, monitor the effectiveness of the program, make changes in the program as appropriate, and publicize its effectiveness to various stakeholders.

An allegation of wrongdoing effectively is a claim that the company's compliance program has failed. This doesn't necessarily mean that it's ineffective; no program can completely prevent wrongdoing. It may mean, however, that if Max is part of the internal investigative team he implicitly may be in the position of evaluating the effectiveness of the program that he has developed and for which he is responsible. This could subtly influence how he assesses the evidence of wrongdoing and evaluates the extent to which deficiencies in the compliance program contributed to misconduct.

In addition, Max's work on compliance makes him the face of the company to many employees. He must earn their trust so that they are willing to follow the compliance program and to let him know when they believe it has been violated and when it needs improvement. Some portion of that trust could be threatened if Max were to assume the role of investigator, gathering evidence that may lead to discipline, termination, and even criminal prosecution of individuals within the company.

Finally, even though Max is a lawyer, not all CCO's are. This means that the compliance office and the CCO may be seen as fulfilling a business, rather than legal, function. This could create ambiguity about whether Max is acting in a business or a legal role when participating in the investigation. Max could be vulnerable to the argument that he is acting as the head of a business unit attempting to determine the extent to which that unit is effectively meeting its objectives for the company. On this argument, only persons working within the general counsel's office are serving as lawyers in conducting the investigation. In this instance, Max is the head of a business unit therefore; Max may be more akin to a client than the company's lawyer in an internal investigation. Max's involvement on the investigative team could jeopardize the availability of the attorney-client privilege and work product protection for employee communications with Max and his documentation of findings.

Furthermore, Max could even be a target or witness as events unfold. Lawyers sometimes presume that as counsel for the company they can't and shouldn't be called as fact witnesses or targeted personally for the actions of employees they can't control. In this instance Max is not only a lawyer but also a compliance officer. This puts him in the position of

carrying business responsibilities for the performance of the compliance team, which a plaintiff or the government may claim that he failed to carry out.

Having said all this, it is not uncommon for a CCO to direct, monitor and investigate compliance issues, and Max's absence from this process could also be a perception problem with the presumed effectiveness of the CCO's office – does it have real authority and the respect of management, or is his "dismissal" from this issue a sign that the compliance function isn't taken seriously and isn't invested in company leadership and decision-making? Another common approach is for the CCO to be an "active consumer" of the outcome of the investigation in which the CCO ensures that a high quality investigation is done, and, if compliance flaws are found, they are promptly remedied.

More generally, the role of lawyers in compliance programs is a current struggle point for many companies. The issue is whether the company's compliance functions should be housed in and report through the legal department (and thus be manned by legal department staff), or whether compliance should be a separate business function, led by a CCO (who may or may not be a lawyer), who has his or her own department and reports directly to management and the Board. Creation of a separate compliance function is always tied to some extent to the law department, in that the compliance department coordinates activities with and makes requests of lawyers in the law department. As a separate department, however, compliance makes decisions that may be just as tied to the perspective of the company's internal audit group and the company divisions they serve, as they are tied to the law department's agenda and modus operandi.

When problems in compliance arise, is it better or worse if the company's lawyers have been integral players in developing, maintaining, measuring, evaluating, improving, and even defending failures in the company's compliance programs? Some would say lawyers can't be positioned (with potential for fatal conflicts) to defend or evaluate that which they create and maintain as business leaders for the company, and others who say that preventive law is the essence of in-house counseling and other functions in the company should report through the legal function to ensure that compliance is done right and in line with legal's perspective. Different companies will have different answers as to which organizational structure works best for them, but this debate has strong implications for the company under a microscope if someone suggests that lawyers are conflicted in their own duties and fiduciary responsibilities as both lawyers and business team leaders.

There is a wide range of practices on this score among companies (with some companies even including an ombudsperson function in the mix), and many opinions on "best practices." However, no matter how the functions are organized, the consensus "best practice" is to ensure that roles are clearly articulated and scrupulously adhered to.

f) Should the investigative report be written or oral? What should it contain? What is "fact" and what is potentially attorney work product protected?

When the company is conducting an investigation that it plans to share with the government, preparing a written report offers certain advantages. The government is likely to regard the company as being cooperative and forthcoming if it has prepared written findings so that the government does not have to rely on the memories of company investigators. Such documentation can also protect the company by avoiding any later claims by employees that counsel misrepresented employee statements or misled persons who were interviewed. In addition, the process of preparing a written report can help sharpen analysis of the information that the investigation has generated, and provides an opportunity to present cogently the company's position of what occurred and why. On the other hand, the preparation of a written report can considerably increase the costs associated with an investigation, and it may be overkill when the matter is relatively simple.

In some circumstances, the "written" report can be a PowerPoint presentation together with attachments or embedded key documents and exhibits. This method allows for a written record of the facts presented to the decision-makers but does not do so with the nuance and "binding" force of a carefully crafted written report. This approach gives the decision-makers more of an opportunity to interact with the investigative team as a remedial approach is developed.

4. If a company receives an allegation against employees whose legal expenses it normally would cover, should it indicate to the government at the outset of an investigation that it will not pay those expenses in order to emphasize the company's willingness to cooperate?

The government may not condition lenient treatment for the company on its refusal to pay attorneys' fees, since the court in *United States v. Stein*, 440 F.Supp.2d 315 (S.D.N.Y.), held that this is unconstitutional. In response to the *Stein* decision, the policy of the DOJ now states: "In evaluating cooperation, . . . 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. Likewise, prosecutors may not request that a corporation refrain from taking such action." United States Attorneys Manual § 9-28.730.

Here the company's decision would not formally be at the request of or a response to pressure from the government. As the General Counsel suggests, however, it is certainly plausible that a prosecutor would informally regard a company's commitment not to pay such fees as an indication of the depth of its interest in cooperating. If the company reasonably fears prosecution, this could be very important. Criminal prosecution could have an especially serious impact on a pharmaceutical company because it likely would reduce public trust in the company and would encourage private lawsuits by third parties claiming civil damages on the side. Furthermore, even if the company ultimately entered into a deferred prosecution agreement, such an arrangement would subject it to intensive monitoring and oversight. Company officers therefore may believe that the corporation must take any feasible steps to avoid criminal charges against the company, and that refusing to pay attorneys' fees is such a step even if it seems like throwing employees over the edge to save the company.

At the same time, should the company commit itself to not paying fees before it has any sense of which officers and employees may or may not be culpable? The unavailability of these fees could effectively deprive these people of the opportunity to defend themselves and even exonerate the company if they are successful in defeating the charges. Furthermore, the perceived disloyalty involved in throwing employees to the wolves in order to save the company may be noted and have a direct impact on employee relations going forward, which the company many not want to lightly discount. Would this seriously undercut morale and future reporting within the company – especially since the DOJ policy precludes the government from considering whether the company is paying attorneys' fees?

These questions are important and company officials may want to think carefully about whether they would be undermining the long-term interests of the company for the sake of a speculative short-term benefit and the optics of finding someone on whom to tag blame that could otherwise land on the company as an entity.

5. Can a company tell employees that it will fire them if they don't cooperate with a company investigation that is conducted at the behest of the government, or whose results will be shared with the government?

Normally, a company has the right to inform its employees that they will be subject to disciplinary action, including termination, if they do not cooperate with a corporation's internal investigation. Some company employee manuals address the issue of investigations and specifically assert that employees must cooperate with company investigations or they can be disciplined up to termination. The company can do so even if the employee is the target of an ongoing grand jury investigation. *Nuzzo v. Northwest Airlines, Inc.*, 887 F. Supp. 28 (D. Mass. 1995).

The complications in this set of facts are that: (1) the company's investigation may be conducted directly at the behest of the government, or (2) the company has already decided that it will turn over the results of its investigation to the government. Under either scenario, the investigation could be deemed the equivalent of an investigation by the government. For the reasons described below, a court might then conclude that employee statements constitute coerced self-incrimination under *United States v. Stein*, 440 F.Supp.2d 315 (S.D.N.Y. 2006).

In *Stein*, the government was conducting a criminal investigation of KPMG. KPMG employees claimed that they had been coerced by the firm to give testimony to the government in its criminal investigation. Specifically, they asserted that KPMG had threatened members who did not make statements to the government with the discontinuation of attorneys' fee payments and termination from the firm. The court found that in two instances members would not have provided testimony to the government in the absence of such threats. In one case, the court said that a defendant "made the statements [the government] at the proffer sessions because KPMG threatened to fire him and cut off payments of his legal fees if he did not." *Id.* at 331. In the other, the court found that the threat to terminate payment of attorneys' fees "left [the defendant] with no practical choice but to cooperate" with the government. *Id.* at 332.

The court held that KPMG's threats in turn were the product of threats by the government against the company. It found that prosecutors told the company that its payment of legal fees would be closely scrutinized, and that they reported to KPMG the identities of employees who refused to make statements with the knowledge that the company "would pressure them to talk to prosecutors." *Id.* at 337. In sum, the court said, the government "coerced KPMG to apply pressure to . . . [the defendants] in order to secure waivers of constitutional rights that the government itself could not obtain." *Id.* at 333. For this reason, the court found that the statements of the two KPMG employees were obtained in violation of their right against self-incrimination.

The *Stein* case involved the constitutional right against self-incrimination, since the statements in question were made *to the government*. In the situation at hand, the company's investigation arguably is "private," and not subject to constitutional constraints. If the company notifies the government and then conducts an investigation at the latter's behest, however, is the company effectively acting as an agent of the government?

Some support for this position is the prosecution of officers of Computer Associates for obstruction of justice for providing false information to a private law firm conducting an internal investigation on behalf of the company. An indictment charged that when the defendants were interviewed by lawyers they "knew, and in fact intended, that the Company's Law Firm would present [the officers'] false justifications to the United States Attorney's Office, the SEC, and the FBI so as to obstruct and impede" the government's investigation in violation of 18 U.S.C. §1512(c)(2). Criminal Information, *United States v. Computer Associates*, Cr. No. 04-837 (ILG) (EDNY), at 14.

If Wilshire conducted an investigation at the direction of the government, employees who were aware of this arrangement could be prosecuted for obstruction of justice under this theory if they provided false information to the company investigators. Does that mean, therefore, that the employees are effectively speaking to the government when they make their statements? If so, they have a right against self-incrimination. Under the reasoning in *Stein*, the company's threat to terminate them for failing to cooperate with the investigation arguably could constitute an impermissible attempt to coerce them to waive a constitutional right.

This argument may be unpersuasive, however, as long as the company and the government can show that the government has placed no pressure on the company to induce employees to talk. Such pressure was the link that established state action, and therefore a constitutional violation, in *Stein*. A court may be reluctant to go even further and find state action simply by virtue of the fact that a company has notified the government of potential wrongdoing, and has agreed to turn over the results of its investigation to authorities. That could substantially expand the scope of state action, and could discourage companies from undertaking investigations at the behest of the government.

The possibility of a coerced waiver of the right against self-incrimination may seem even less likely when a company conducts an investigation and approaches the government only at the end of that process. The government has been unaware of the investigation, and therefore has not been in position to exert any pressure on the company. While the company's desire to win favor with authorities may create an incentive to threaten dismissal of any employee who

fails to cooperate, that seems too indirect a link to constitute governmental coercion. Finally, the mere fact that the company intends to turn the results of its investigation over the government may not in itself transform the company into a state actor for constitutional purposes.

6. When a company is preparing to conduct a confidential investigation of alleged wrongdoing, what public comments can an officer make if faced with questions that relate in some way to the subject matter of the investigation?

In this case, the risk for the CEO is that he may commit securities fraud under SEC Rule 10b-5 by making materially misleading statements or by omitting material information necessary to ensure that what he says is not misleading. There is also arguably a risk to the CLO who does not warn him about his disclosure responsibilities or persuade him to fully treat the issue in accordance with what 20/20 hindsight will deem to be reasonable.

The allegation that Nolip data were falsified has not been confirmed, so it would be premature – and potentially quite harmful to the company – to say anything about that allegation at this point. At the same time, the CEO knows that there is some reason at least to question whether the drug is completely safe and to know that there could be a substantial financial impact in the future. For that reason, the CEO may want to avoid making any unqualified statements about the safety of Nolip.

The CEO may want to confine any remarks about Nolip to the specific incident in which the woman recently died. The CEO can perhaps say that there is no conclusive evidence at this point about the reason for her death, and that the company is ready to cooperate in any inquiry about the circumstances surrounding it. Any other comment he can say, may be premature at this time.

References & Resources

Ethics Rules

ABA Model Rule 1.6: Confidentiality of Information
ABA Model Rule 1.7: Conflict of Interest: Current Clients
ABA Model Rule 1.13: Organization as Client
ABA Model Rule 3.7: Lawyer as Witness

Statutes and Regulations

17 C.F.R. § 205: Standards of Professional Conduct for Attorneys Appearing and Practicing before the Commission in the Representation of an Issuer

Securities Exchange Act of 1934, 15 U.S.C. § 78u-6 (Securities whistleblower incentives and protection)

Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, Release No. 34-64545

False Claims Act, 31 U.S.C. § 3730 (h) (Relief from retaliatory actions)

Sarbanes-Oxley Act, 18 U.S.C. § 1514A (Civil action to protect against retaliation in fraud cases)

Commodity Exchange Act, 7 U.S.C. § 26 (Commodity whistleblower incentives and protection)

Final Rules Implementing the Whistleblower Provisions of Section 23 of the Commodity Exchange Act, 76 FR 53172

Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. 5567 (Employee protection)

Consumer Financial Protection Bureau Bulletin 2011-05 (Enforcement and Fair Lending), Subject: Bureau Invites Whistleblower Information and Law Enforcement tips and Highlights Anti-

Restatements

Restatement (Third) of the Law Governing Lawyers §96: Representing an Organization as Client

Books

John Villa, *Corporate Counsel Guidelines*

Barry F. McNeil & Brad D. Brian, Internal Investigations (3d. ed. 2007)

Dan K. Webb, Robert W. Tarum & Steven F. Molo, *Corporate Internal Investigations* (2007)

Kaye Scholer LLP, *Deskbook on Internal Investigations, Corporate Compliance and White Collar Issues* (2007)

Milton C. Regan, Jr. & Jeffrey Bauman, *Legal Ethics in Corporate Practice*, Chapter 24: Internal Investigations, p. 1014 (2005)

Gary H. Collins & David Z. Seide, *Warning the Witness: A Guide to Internal Investigations and the Attorney-Client Privilege* (2010)

Kirk Ogrosky, *Recent Developments Impacting the Investigation, Enforcement, and Defense of White Collar Criminal Activity in the Healthcare Arena, Managing White Collar Legal Issues (Inside the Minds)* Ch. 3 (2012)

Articles

Colin P. Marks, *Internal Investigations: Ethical Concerns of the "Deputized Counsel,"* 38 St. Mary's L. J. 1065 (2007)

Robert R. Stauffer & Thomas Monroe, *Internal Investigations: Conducting Employee Interviews After Stein and the McNulty Memorandum,* BNA CORPORATE ACCOUNTABILITY REPORTER, Vol. 5, No. 14, April 6, 2007

Sarah Helene Duggin, *Internal Corporate Investigations: Legal Ethics, Professionalism and the Employee Interview*, 2003 COLUM. BUS. L. REV. 859 (2003)

Robert R. Stauffer & Thomas Monroe, *Internal Investigations: Conducting Employee Interviews After Stein and the McNulty Memorandum,* BNA CORPORATE ACCOUNTABILITY REPORTER, Vol. 5, No. 14, April 6, 2007

Timothy P. Harkness & Darren LaVerne, *Lying to In-House Counsel May Lead to Prosecution*, NAT. LAW J., July 27, 2006

Lawton P. Cummings, *The Ethical Minefield: Corporate Internal Investigations and Individual Assertions of the Attorney-Client Privilege,* 109 W. Va. L. Rev. 669 (2007)

Elizabeth C. Tippett, *The Promise of Compelled Whistleblowing: What the Corporate Governance Provisions of Sarbanes Oxley Mean for Employment Law*, 11 Empl. Rts. & Emply. Pol'y J. 1 (2007).

Peter C. Kostant, *From Lapdog to Watchdog: Sarbanes-Oxley Section 307 and a New Role for Corporate Lawyers*, 52 N.Y. L. Rev. (2007/08)

Dave Ebersole, *Blowing the Whistle on the Dodd-Frank Whistleblower Provisions*, 6 Entrepren. Bus. L.J. 123 (2011)

Heather Jones, *The Dodd-Frank Whistleblower Program: An Analysis of the Proposed & Final Rules,* 2 Am. U. Labor & Emp. L.F. 131 (2011)

Pamela Bucy Pierson & Anthony A. Joseph, *Corporate Compliance: Creating An Effective Corporate Compliance Plan: Part II*, 72 Ala. Law. 284 (2011)

Shannon Kay Quigley, *Tug-of-War: Corporate Attempts to Secure Internal Reporting Procedures in the Face of External Monetary Incentives Provided by the Dodd-Frank Act*, 52 Santa Clara L. Rev. 255 (2012)

Jenny Lee, *Corporate Corruption & the New Gold Mine HOW THE DODD-FRANK ACT OVERINCENTIVIZES WHISTLEBLOWING*, 77 Brooklyn L. Rev. 303 (2011)

Corporate Board Member, *Talking Points: Impact of Whistleblower Rules on Internal Investigations* (June 2011)
http://www.boardmember.com/Article_Details.aspx?id=6362

Cases

United States v. Stein, 440 F.Supp. 315 (S.D.N.Y. 2006)

In re Qwest Communications Int'l. Inc. Securities Litigation, 450 F.3d 1179 (10th Cir. 2006)

In re Columbia/HCA Healthcare Corp. Billing Practices Litigation, 293 F.3d 289 (6th Cir. 2002)

Westinghouse Electric Corp. v. Republic of the Philippines, 951 F.2d 1414 (3d. Cir. 1991)

In re Steinhardt Partners, L.P., 9 F.3d 230 (2d. Cir. 1993)

Upjohn v. United States, 449 U.S. 383 (1981)

Commodity Futures Trading Commission v. Weintraub, 471 U.S. 343 (1985)

United States v. Hart, 1992 WL 348325 (E.D. La. 1992)

Westinghouse Electric Corp. v. Kerr-McGee Corp., 580 F.2d 1311 (7th Cir. 1978)

United States v. Ruehle, 583 F. 3d 600 (C.D. Cal. 2009)

Lewis v. Wells Fargo & Co. 266 F.R.D. 433 (N.D. Cal., 2009)

Cason-Merenda v. Detroit Med. Ctr., 2010 U.S. Dist. LEXIS 103462

Lerman v. Turner, 2011 WL 62124 (N.D. Ill. 2011)

ACC Resources

Advocacy:

- *Dodd-Frank Whistleblower Bounty Provisions- ACC Comments Letter to House Financial Services Committee* (May 2011)
  http://www.acc.com/legalresources/resource.cfm?show=1282662

- *Dodd-Frank Whistleblower Bounty Program-ACC Comments Letter Draft* (December 2010)
  http://www.acc.com/legalresources/resource.cfm?show=1224290

- *Dodd-Frank Whistleblower Bounty Program-ACC 1 pager* (November 2010)
  http://www.acc.com/legalresources/resource.cfm?show=1210897

Presentations:

- *Whistleblower Training Course* (WeComply, Inc.)
  http://www.acc.com/legalresources/resource.cfm?show=1278762

- *Avoiding Retaliation Training* Course (WeComply, Inc.)
  http://www.acc.com/legalresources/resource.cfm?show=1278069

- *Whistle While You Work 3.0-New Tunes for Whistle Blower Protections and Employment Retaliation Claims* (Jim Beyer, Ellen Malasky, William Mordan)
  http://www.acc.com/legalresources/resource.cfm?show=1302786

- *Whistleblower and Where the Government Gets Their Information* (Sarena Straus)
  http://www.acc.com/legalresources/resource.cfm?show=1302811

- *Whistleblower Cases and Lessons Learned* (Pamela W. Popp)
  http://www.acc.com/legalresources/resource.cfm?show=1302816

- *SEC Adopts Final Rules on the Dodd-Frank Whistleblower Program-But Is This a Game Changer?* (W. Scott Sorrels)
  http://www.acc.com/legalresources/resource.cfm?show=1304092

- *How to Survive a SOX Whistleblower Complaint* (Roscoe C. Howard Jr., Tanya Axenson Macallair, and Dean A. Manson)

http://www.acc.com/legalresources/resource.cfm?show=164465

- *Whistleblower/Internal Investigations & How to Respond to the SEC* (Meric Craig Bloch, Kerry A. Galvin, and Kim Rivera)
  http://www.acc.com/legalresources/resource.cfm?show=20122

Top Ten:

- *Top Ten Considertaions for Whistleblowing Schemes in Europe* (ACC with contributions from Phillip W. Turner)
  http://www.acc.com/legalresources/publications/topten/whistleblowing-scheme-in-europe.cfm

QuickCounsel:

- *An Overview of Federal Whistleblower Regulations* (Rachel Okolski, Esq. for ACC)
  http://www.acc.com/legalresources/quickcounsel/whistleblowing.cfm

InfoPAK:

- *Management and Defense of Employee Whistleblower Claims* (Jackson Lewis LLP)
  http://www.acc.com/legalresources/resource.cfm?show=640082

- *Building and Developing Compliance Programs: Preparing and Protecting Your Organization*
  http://www.acc.com/legalresources/resource.cfm?show=1316835 (Holland & Knight)

- *Internal Investigations* http://www.acc.com/legalresources/resource.cfm?show=19675
  (Morrison Foerster)

- Crisis Management in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in A Global Environment
  http://www.acc.com/legalresources/resource.cfm?show=77428 (Skadden)

Samples:

- *Model Association Whistleblower Policy #2* (Venable)
  http://www.acc.com/legalresources/resource.cfm?show=141640

- *Model Association Whistleblower Policy #3* (Venable)
  http://www.acc.com/legalresources/resource.cfm?show=141604

- *Sample Whistleblower Policy* (ACC)
  http://www.acc.com/legalresources/resource.cfm?show=12427

- *Whistleblower Policy Statement*
  http://www.acc.com/legalresources/resource.cfm?show=12737

- *Whistle Blowing Policy and Procedures*
  http://www.acc.com/legalresources/resource.cfm?show=13909

- *Enforcement of Standards and "Whistleblower" Protections*
  http://www.acc.com/legalresources/resource.cfm?show=13912

Quick Reference:

- *Nine Items to Remember to Avoid Complications from the Dodd-Frank Whistleblower Provisions*
  http://www.acc.com/legalresources/resource.cfm?show=1303974

Webcasts:

- *Responding to the Dodd-Frank Whistleblower Program* (ACC's Corporate & Securities Law Committee)
  http://webcasts.acc.com/detail.php?id=511979&go=1

- *Understanding and Reporting to Whistleblower Reports* (ACC's New to In-house Committee and Sponsored by Bass, Berry, & Simms, PLC)
  http://webcasts.acc.com/detail.php?id=595050&go=1

- *SOX Whistleblower Claims: A Sixth Anniversary Survival Guide* (Greg Watchman, Richard Cino, and Stanley Keller)- Transcript of Webcast
  http://www.acc.com/legalresources/resource.cfm?show=139201

- *Whistleblower Anonymous Hotlines and SOX-Dealing with the French and German Decisions* (Carol Seaman, Paula Barrett, Christel Cacioppo, and Constanze Hewson)- Final transcript of Webcast
  http://www.acc.com/legalresources/resource.cfm?show=16412

ACC White Paper:

- *Lawyers as Whistleblowers: The Emerging Law of Retaliatory Discharge of In-House Counsel* (Lucian Pera and ACC), http://www.acc.com/legalresources/resource.cfm?show=16079-

Other Resources

"Principles of Federal Prosecution of Business Organizations," Memorandum from Mark R. Filip, Deputy Attorney General, to Heads of Department Components and United States Attorneys (Aug. 28, 2008) *available at* http://www.usdoj.gov/opa/documents/corp-charging-guidelines.pdf.

Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions ("Seaboard Report"): http://sec.gov/litigation/investreports.shtml

U.S. Sentencing Guidelines Manual, Chapter 8: Sentencing of Organizations:
http://www.ussc.gov/Guidelines/2011_Guidelines/Manual_HTML/Chapter_8.htm

Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

InfoPAK[SM]

Internal Investigations

Sponsored by:

MORRISON | FOERSTER

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

Internal Investigations

August 2012

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This InfoPAK℠ is designed to assist in-house counsel in the design and execution of internal investigations. It discusses how to structure the investigation, manage documents, conduct interviews, and communicate about the investigation with third parties, such as auditors and regulators. This InfoPAK℠ also provides guidance on specific topics such as the risks associated with cross-border investigations, indemnification and insurance, and maximizing the investigation's privilege protections.

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 Morrison & Foerster or of ACC or any of their lawyers, unless so stated. Further, this InfoPAK is not intended as a definitive statement on the subject. Rather, it is intended to serve as a tool for readers, providing practical information to the in-house practitioner.

This material was authored by Morrison & Foerster, the 2012 ACC Litigation Committee Co-Sponsor, under the direction and guidance of the ACC. For more information, please see the "About the Author" section of this InfoPAK or visit www.mofo.com.

Contents

I. Introduction

A. What Is An Internal Investigation?

An internal investigation is the development and analysis of facts by an organization that will form the basis for a decision by that organization.

This InfoPAK addresses the complex problems that can arise during an investigation. It discusses the events that can trigger an investigation, the corporate governance considerations informing the selection of an investigation team, the collection, preservation, and analysis of documents, and the daunting privilege and disclosure issues that often arise.

This InfoPAK begins, however, with the real end in sight. The internal investigation is not only—and perhaps not even primarily—about "getting to the bottom of things." It is not an exercise in learning for learning's sake. Nor is it the investigation's aim to compile evidence so that some third party (like an auditor or regulator) can render a decision. The true reason-for-being of the internal investigation is something else.

The key phrase in the definition is "*decision by that organization*." The internal investigation is a prelude to a corporate decision. That decision could be a personnel action, a restatement of the financials, or a disclosure that leads to enterprise-threatening litigation or criminal prosecution. It is the nature of that decision that will shape how the investigation is conducted and will ultimately inform many of the tough judgments to be made during the process.

Of course, as the investigators develop new facts, the decision to be made at the end of the process will change (*e.g.*, what looked at first like it was going to be a decision on personnel action is now looking like a decision as to whether to self-report an antitrust violation and seek amnesty). As the investigation's purpose changes, its scope (and thus procedures) must evolve accordingly. In other words, the investigators must constantly reassess scope and procedures in light of the facts they discover.

B. Preparing For The Next Internal Investigation

1. Uses For This InfoPAK

This InfoPAK explains the complexities of internal investigations and seeks to provide an appreciation of the benefits to a company of a properly done investigation (or, alternatively, the costs of an investigation improperly done). At the same time, each section is meant also to be a stand-alone resource.

Section II describes how company events may trigger the need to conduct an internal investigation. Section III explains how to structure and staff the investigation in compliance with corporate governance requirements. Section IV is about documents: the challenges of preserving them, and efficiently collecting and reviewing them. Section V covers a critical part of the investigation—interviews. If the investigation has any cross-border dimension, Section VI will help to avoid inadvertently running afoul of other countries' laws. Section VII explains typical

real-time communications about an investigation with third parties such as auditors, the government, or the stock market. Section VIII covers indemnification and insurance—who will pay for the investigation and what will they pay for? Section IX discusses how to wrap up the investigation—formulating the findings and conclusions, deciding how best to memorialize and report them, and implementing any remedial measures. The InfoPAK ends with Section X's discussion of how to maximize the investigation's privilege protections.

2. Preparing An Internal "Playbook"

This InfoPAK should serve as a companion to an organization's own internal playbook. Think of the playbook as a plan in place if and when the need for an investigation arises. It obviously should be tailored to each organization. Some things a useful playbook might contain are contact information for key internal people who may need to be involved, information for key IT personnel and vendors, and the latest data map (describing server or network topology), company policies and procedures related to whistleblower tips and complaints, human resources policies, and collective bargaining agreements.

II. When To Conduct An Internal Investigation

A. What Triggers Internal Investigations?

Investigations are often triggered by allegations of misconduct. But a company cannot launch an inquiry every time it is the subject of a short seller report or unflattering blog post. How, then, does one decide what merits further inquiry?

There is no simple answer to that question. But it generally depends on:

- The nature and gravity of the allegation;
- The source and circumstances under which the organization received the allegation; and
- The extent to which the allegation has been corroborated.

With that in mind, consider these seven common internal investigation triggers:

1. Whistleblower Complaints

Whistleblowers have spawned an ever-larger proportion of internal investigations. That is probably due to changes in the law over the last decade. In the wake of the Enron scandal, which itself began with a whistleblower, Congress required public company audit committees to establish procedures by which employees could anonymously raise complaints about "questionable accounting or auditing matters."[1] In response, companies established anonymous whistleblower telephone hotlines or e-mail addresses.

Of course, would-be whistleblowers often bypass hotline processes entirely, instead lodging complaints with colleagues, supervisors, and union representatives. Indeed, the whistleblower may take his complaint directly to regulators. Under the Dodd-Frank Act, an individual who voluntarily provides "original information" to the U.S. Securities & Exchange Commission ("SEC") about a "possible violation" that leads to a sanction of least $1 million will receive a cash bounty of between 10 and 30 percent of the money collected.[2] Although the SEC says that it may reward whistleblowers who participate in their company's internal compliance process, employees are under no obligation to speak to their company first.

However the organization learns of a complaint, and whatever management thinks of the complaint's merits, whistleblowers must be handled with care. Both the Sarbanes-Oxley Act of 2002 and Dodd-Frank Act protect whistleblower employees against retaliation. Sarbanes-Oxley makes it unlawful for a company, its agents, or employees, to "discharge, demote, suspend, threaten, harass or in any other manner discriminate against an employee" in retaliation for providing information about a possible violation of the federal securities laws.[3] The Dodd-Frank Act includes similar protections, though it applies to all companies, regardless of whether they are publicly traded, and protects a broader range of whistleblower conduct.[4] An employee who alleges retaliation in violation of Sarbanes-Oxley or Dodd-Frank may bring an enforcement action against the company in federal court seeking reinstatement, back pay, and other compensation.[5] Some states have their own laws protecting whistleblowers.[6]

2. Internal Requests For Guidance

The investigation triggers from within an organization are not always styled as complaints of misconduct. A seemingly routine question from the field, anomalous transaction, or unexpected business reversal can require follow-up. For example, unsatisfying explanations for a customer's refusal to pay down a receivable may lead a finance team to question whether revenue recognition was proper last quarter. Or a new sales operations manager could report that a member of her staff was asked to pay a small gratuity to clear foreign customs and ask whether her predecessor accommodated such requests. Wise in-house counsel know that today's apparently isolated incident, if ignored, can be tomorrow's missed red flag.

3. Government Investigation

In simpler times, after learning that her company was under government investigation, in-house counsel would simply engage a law firm to prepare the company's defense. Today, however, in-house counsel will often weigh conducting an internal investigation into the challenged conduct. That's because, if there is ongoing illegal conduct, counsel, the Board of Directors, and management must stop it right away. Moreover, as discussed in Section II.C, *infra*, an investigation may ultimately win the company leniency. Even where the government has simply requested information and remains otherwise circumspect about the purpose, source, or focus of its inquiry, the organization will likely need to conduct some factual investigation to respond.

4. Auditor Inquiry

Questions and reports from auditors also prompt many internal investigations. Although auditors may flag a clear indication of fraud, the triggers are more commonly as simple as a question about

the purpose of a payment, a request for the support for an accounting entry, or the refusal of a customer to return a confirmation request.

Failure to investigate in response to an auditor inquiry can have severe consequences, including the resignation of the auditors and a report to the SEC. Under Section 10A of the Securities Exchange Act of 1934, when an auditor learns information indicating that it is likely that an illegal act has occurred, the auditor must determine the possible effect on the financial statements, inform the appropriate level of management, and assure that the audit committee has been informed.[7] If the company fails to investigate and remediate appropriately, and the auditor concludes that the misconduct would have a material effect on the company's financial statements and would warrant departure from a standard auditor's report, the auditor must report the misconduct directly to the company's Board. The Board must then immediately inform the SEC of the report. If it does not, the auditor must inform the SEC of the report and may resign from the engagement.[8] Obviously, it is far preferable to avoid this sequence of events with a prompt, thorough investigation.

5. Civil Litigation

Almost any type of civil litigation (including commercial or securities fraud, price fixing, and product liability) can trigger an internal investigation. That is peculiarly true of shareholder derivative litigation, which is brought by a shareholder on behalf of the corporation itself. A pre-litigation shareholder demand may prompt a Board to investigate. Or, after derivative litigation has commenced, a company's board of directors may attempt to assume control of the litigation by forming a "special litigation committee" of disinterested directors charged with investigating the claims.[9] If the committee determines that the claims are meritorious, it can settle or allow the derivative litigation to proceed.[10] If the committee finds that the claims lack merit, it can seek dismissal. Courts defer to the conclusions of a special litigation committee where the special litigation committee establishes that there are "no genuine issues of material fact as to its independence, the reasonableness and good faith of its investigation, and that there are reasonable bases for its conclusions."[11]

6. Complaints Of Harassment

Although an employer may be vicariously liable for sexual harassment of which it was not aware, it may avail itself of an affirmative defense if it can show:

1. That the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and
2. That the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.[12]

To meet the first prong, a company can demonstrate its reasonable care by both propounding an anti-harassment policy and promptly investigating and correcting the misconduct.[13]

7. Media Reports

Media reports questioning conduct at a company or within an industry sometimes trigger investigations. The *Wall Street Journal*'s "The Perfect Payday" article, published on March 18, 2006, concerning the back-dating of stock option grants for company executives, is perhaps the most prominent example. It ultimately inspired hundreds of internal investigations.

B. Who Decides Whether To Investigate?

In-house counsel may be the first to receive an allegation or question suggesting a need for further investigation, but counsel may not be the final decision maker as to whether and how to respond. Many companies have adopted protocols requiring certain claims to be escalated to particular members of senior management or the Board of Directors.[14] Playing an operational, decision-making (rather than advisory) role may jeopardize privilege and be perceived to impair in-house counsel's impartiality.

In some cases, moreover, SEC regulations dictate that counsel "report up" within the organization. Generally speaking, these obligations come into play when an attorney representing an issuer becomes aware of credible evidence of a material:

- Violation of federal or state securities laws;
- Breach of fiduciary duty arising under those laws; or
- Violation of any similar U.S. federal or state law.[15]

An attorney's federal "reporting up" obligations rest on whether the attorney is "supervisory" or "subordinate." A supervisory attorney has these "reporting up" options:

- Report the evidence to the chief legal officer of the company (the "CLO") or to both the CLO and the CEO. If the attorney does not "reasonably believe" that this results in an "appropriate response" "within a reasonable time," she must make a report to the company's audit committee (or, if the company has no audit committee, then to another committee consisting of directors not employed by the company, and if no such committee exists, to the full Board).[16]
- If counsel believes that it would be futile to report to the CLO or the CEO, they then report the evidence to the company's audit committee (or, if the company has no audit committee, then to another committee of the Board consisting of directors employed by the company, and if no such committee exists, to the full Board).
- Report the evidence to a "qualified legal compliance committee" (a "QLCC").[17] A QLCC must have the authority to investigate and report evidence of material violations. Once counsel reports the violation to the QLCC, she is not responsible for assessing whether the issuer's response was appropriate.[18]

A subordinate attorney must report evidence of a material violation to her supervising attorney.[19] If she reasonably believes that her supervisory attorney failed to comply with the reporting options discussed above, she may (but is not required to) avail herself of the reporting options available to a supervisory attorney.[20]

C. Why Should A Company Investigate?

What factors should the person or committee charged with deciding whether to investigate consider? On the one hand, investigations are often expensive, disruptive, and, if disclosed, can have a negative impact on the company's stock price and reputation. They may also trigger (and undermine the company's position in) shareholder, commercial, and employment litigation. What factors, then, might weigh in favor of investigation? Consider these six:

1. Stop Misconduct From Damaging The Business

Whether misconduct violates federal or state law, or merely a company's internal policies and procedures, chances are it is having an adverse effect on the company's business. An investigation is usually a prerequisite to finding and stopping misconduct, and limiting the company's exposure.

2. Internal Compliance Programs And Codes Of Conduct

A company's internal compliance program or code of conduct may *require* an internal investigation. Ignoring company policy may suggest that the organization has been, at best, careless in its overall legal compliance or, worse, that management has turned a blind eye to obvious wrongdoing. In this way, ignoring company policies requiring investigation can undermine a company's civil litigation posture and enhance the risk of prosecution.

3. Law Enforcement Incentives

A prompt investigation is one factor that regulators and law enforcement will consider in determining whether and how severely to sanction a company for wrongdoing. Not only can a comprehensive internal investigation result in leniency, it is indispensable if a company intends to seek full cooperation credit.

The best-known articulation of the government's cooperation policy is the "Seaboard Report," in which the SEC explained its rationale for declining to sue a company, even though the company's periodic reports had been misstated and its books and records inaccurate in violation of the Securities Exchange Act of 1934.[21] Among the several factors the SEC cited was the fact that, within a week of being notified of potential misconduct, the Board of Directors had hired an outside law firm "to conduct a thorough inquiry." In weighing a company's response to an indication of wrongdoing, the SEC said that it asks a number of questions, including:

- Did the company commit to learn the truth, fully and expeditiously?
- Did it do a thorough review of the nature, extent, origins and consequences of the conduct and related behavior? . . .
- Were scope limitations placed on the review? If so, what were they?[22]

A thorough internal investigation is a prerequisite to several of the Seaboard Report's other mitigating factors, such as remediation, self-reporting, and sharing investigative materials with the enforcement staff.

Similarly, the Department of Justice's ("DOJ") corporate charging guidelines, most recently described in the "Filip Memorandum," hold out the prospect of credit to corporations that promptly self-police, self-report, and remediate.[23] DOJ's Antitrust Division goes even further. Its Corporate Leniency Policy provides that a corporation involved in illegal antitrust activity will not be charged if it reports the illegal activity to the Antitrust Division before the Division is notified by any other source (and if the company fully cooperates with the Antitrust Division and meets certain other conditions).[24] And even where a company cannot avoid criminal prosecution, Chapter Eight of the Federal Sentencing Guidelines provides that

The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.[25]

4. Director And Officer State Law Duties

Directors have a responsibility to conduct a proportionate and effective investigation when faced with a credible allegation of wrongdoing at the company. If they fail to do so, they face the possibility of personal liability.[26] That's because they owe a duty of care, including the duty to establish a system to prevent (and if necessary correct) criminal misconduct. *In re Caremark Int'l Inc. Derivative Litig*.[27] The *Caremark* court relied in part on the federal Sentencing Guidelines (discussed above), which "offer powerful incentives for corporations today to have in place compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to take prompt, voluntary remedial efforts."[28] The court further stated, "Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development and the enhanced penalties and the opportunities for reduced sanctions that it offers."[29]

5. Certifications

Sarbanes-Oxley requires that certain public filings made pursuant to the Securities Exchange Act of 1934 include a signed certification from the issuer's CEO and CFO. These certifications must state, among other things, that the filing does not contain any material misrepresentation or omission and that the company has sufficient internal controls.[30] Filing a false certification can expose corporate officers to an SEC enforcement action and even criminal charges.[31] Accordingly, CEOs and CFOs rightly decline to sign certifications where a company has failed to investigate allegations of internal misconduct.

6. Adverse Publicity And Pressure From Customers

Unanswered questions about possible misconduct can damage a company's reputation with shareholders and customers. Many companies find that uncertainty—whether about the company's products, practices, financial results, or viability—is more damaging than a confirmed

negative fact. Refuting a rumor, or simply confirming and addressing it, requires a credible investigation.

7. Remediation

Remediation is the indispensible cornerstone to satisfying most internal compliance policies, receiving credit from regulators and law enforcement, meeting director obligations, permitting officer certifications, and addressing shareholder or customer concerns. Until a company has investigated, it cannot credibly remediate.

D. Scope And Work Plan

1. Identifying The Scope

Much of what has been written about internal investigations urges the practitioner to "set an appropriate scope." But how does one do that? The introduction defined the internal investigation as the development and analysis of facts from within an organization that will form the basis for a decision by that organization. The investigators, then, should adopt a scope reasonably calculated that will allow the organization to make the decision it ultimately needs to make. Of course, as noted above, the nature of the decision to be made by the organization may change as the investigators learn new facts, and so the scope should change accordingly.

2. Work Plan

Establish a work plan at the outset that reflects the investigation's scope, but remember it is a "living document" that will evolve as the investigation develops. Law enforcement and auditors will likely expect a company to have a work plan early on so that they can assess the sufficiency of company procedures. Identify the major tasks, who will be responsible for them, and estimate when each will be completed. These tasks will include document preservation, collection, and review, interviews, and analysis, all of which are discussed in the chapters to come.

Consider preparing a preliminary budget to enable planning by finance personnel. Also, take note of anticipated deadlines, such as SEC filing dates and obligations to debt holders. Neither the budget nor external deadlines, however, should determine the procedures ultimately conducted. At the end of the investigation, those conducting the investigation must be able to report that they did all the work reasonably called for by the investigation's scope, and that they took the time necessary to perform those procedures with appropriate diligence.

Finally, there are several questions that should be revisited throughout the investigation. They may be unanswerable at the beginning, but they remain important:

- Do the investigators need expert help, such as forensic accountants, an industry expert, or a handwriting expert?

- Do any of the witnesses need counsel? Sometimes, subject to various ethical obligations, a single counsel can represent multiple witnesses. Consider identifying such "pool counsel" early.
- Do the investigators face cross-border issues implicating foreign employment, data privacy, or data transfer laws?
- Does the organization need outside legal advice about contemplated remedial measures, such as employment counsel to advise about disciplinary action?

III. Who Should Supervise And Conduct The Investigation?

Once the organization has decided that it needs to conduct an internal investigation, it faces important decisions about who should manage and conduct the investigation. This section addresses the issues that the organization should consider when making those decisions. One of the most important considerations is the likely effect on the credibility of the investigation. Unless the investigation is viewed as credible—by third parties such as government regulators, prosecutors, auditors and investors, and by individuals within the organization who will have to make business decisions based on the results of the investigation —the organization will not obtain the benefits it hoped to achieve when it decided to initiate the investigation.

A. Supervision: Management Or The Board?

In some cases, the decision about who should supervise the internal investigation flows directly from the reasons for conducting the investigation. If the allegations or suspected misconduct triggering the internal investigation involve management, then management should not be in charge of the investigation. An investigation carried out by management in such situations is not likely to be considered credible.

When the allegations do not involve management, the company must carefully consider the need for independence, both in fact and in appearance. Among third parties—especially government regulators and prosecutors—there is often a perception that supervision by management can compromise the independence of the investigation. For example, management may have an interest in minimizing the problems found by the investigators, leading to inappropriate limitations on scope.

When the subject of the internal investigation is sensitive or suggests illegal activity or other corporate malfeasance, the investigation should be supervised by a committee of the Board consisting of independent outside directors. For public companies, the committee will often be the company's Audit Committee. At least since Sarbanes-Oxley, audit committees of public companies have the authority to engage independent counsel and other advisers in connection with their oversight duties. If another committee is taking the lead, the Board should pass a resolution broadly authorizing the committee to conduct the investigation, retain counsel and consultants, and report its findings to the full Board.

B. Choosing The Investigator

The choice of investigator may depend on the nature of the allegations triggering the internal investigation. Non-lawyer compliance officers and internal audit departments with staff are often quite capable of handling internal investigations. Such investigations may focus on assessing compliance with company policies and improvement of internal controls.

For most serious allegations—especially allegations that could result in criminal prosecution, civil lawsuits, or regulatory enforcement actions—attorneys with investigative experience and familiarity with applicable law should be chosen to conduct the investigation. Using lawyers will help ensure that the investigation is protected by the attorney-client privilege. Although, as discussed below, the organization may ultimately elect to waive the privilege, maintaining the privileged nature of the investigation by using counsel will give the company the flexibility to make such decisions for itself.

1. In-House Counsel Or Outside Counsel?

Many companies have sophisticated legal departments with the capability to handle investigations internally. When that is the case, having in-house conduct the investigation can be less expensive than using outside counsel and, because in-house counsel is more familiar with the company, the industry, and the relevant individuals, more efficient.

Notwithstanding these benefits, it is sometimes in the best interests of the company to rely on outside counsel. Outside counsel may be perceived to be more independent and objective because they are less involved with the company's programs and personnel. This is especially true when the activities of in-house counsel's colleagues may be the subject of the investigation, or when business decisions that involved in-house counsel are examined.

In addition, the risk to the attorney-client privilege is higher for in-house counsel than for outside counsel because in-house counsel are frequently called upon to provide business as well as legal advice with respect to matters under investigation. And in-house counsel may prefer not to be put in the position of having to decide whether to disclose information to a prosecutor, to recommend discipline for culpable employees, or to explain how and why violations were committed in the first place. Further, in the event a lawyer must later testify about the investigation, in-house counsel may prefer to assign outside counsel the role of witness.

Even when outside counsel is selected to conduct the internal investigation, in-house counsel still have an important role to play. Their knowledge of the company is a valuable resource to outside counsel, and the company will continue to rely on in-house counsel's advice.

In summary, an internal investigation that involves matters unlikely to interest regulators or prosecutors is often more suitable matter for a legal department to handle fully. But in cases where the alleged wrongdoing is pervasive, may have occurred at high levels, or is likely to come to the attention of regulators or prosecutors, consider engaging outside counsel.

2. Regular Outside Counsel Or Special Counsel?

If an organization decides to hire outside counsel, it must next determine whether to engage a firm with which it has a preexisting relationship. As with in-house counsel, regular company counsel will be more familiar with the company's business and personnel. Consequently, regular outside counsel may be able to conduct the investigation more efficiently than special counsel. That may be important where the organization needs immediate information to make quick decisions.

On the other hand, regular counsel are less independent. In some situations, regular counsel may have been rendered legal advice connected to the investigation's subject matter or may have participated in relevant transactions. Indeed, a lawyer from a company's outside firm may even be interviewed as a witness during the investigation. Further, regular counsel may have long-standing allegiances to individuals and may be dependent on management for future legal work. Hiring a new law firm, not perceived to be beholden to management and not entangled in the underlying facts, can give the internal investigation added credibility. This is especially important in the face of potential criminal or regulatory enforcement action.

3. The Role Of Outside Consultants

Often investigators will benefit from hiring consultants to assist them, including:

- Forensic accountants, who can provide a better understanding of the applicable accounting rules and concepts and who are trained to detect irregularities;
- e-discovery consultants, who can provide technical expertise and support in managing and reviewing electronic data;
- Subject matter consultants, who can be helpful in identifying issues in complex industries.

Consultants can increase the likelihood of detecting potential problems and potential defenses. In many circumstances, the expense of hiring consultants is more than offset by the resulting efficiencies. And qualified, independent outside consultants will often enhance the credibility of an investigation among third party consumers of the results, such as auditors, regulators, investors, and courts.

When counsel conducts the investigation, the work of outside consultants may be privileged. *United States v. Kovel* provides the legal framework regarding extension of the attorney-client privilege to the work outside consultants.[32] Experts should be hired by counsel and sign retention agreements that make clear their engagement is in contemplation of providing assistance for legal advice.

IV. Document Preservation, Collection, And Analysis

Whatever the subject matter of the investigation, documents are critical. They usually provide the most reliable source of facts and serve to refresh witness memories. This section introduces the critical and recurring issues related to the preservation, collection, and review of documents during an internal investigation.

A. Preservation Of Evidence

1. The Obligation To Preserve Evidence

It is essential that an organization initiate preservation efforts immediately upon deciding that an internal investigation is necessary. Preservation is not just a prerequisite to a thorough investigation, it is also mandated by law and counsel's professional responsibilities.[33] The duty to preserve evidence is triggered when a party knows or should know that the evidence is relevant to a pending, future, or merely "foreseeable" litigation or government investigation.[34] The failure to do so can have severe consequences. Companies and individuals can be punished for spoliation where relevant documents are lost or destroyed.[35] Criminal charges may be filed for obstruction of justice, and civil penalties may be imposed.

In recent years, it has become easier for the government to prosecute document destruction. Until 2002, to establish obstruction of justice, the government was required to prove interference with a *pending* governmental investigation.[36] That is no longer the case. Sarbanes-Oxley criminalized the knowing destruction or alteration of evidence occurring even before a governmental investigation is commenced.[37] The statute applies to both public and private companies, as well as individuals. Courts have recently upheld convictions where a government investigation was "foreseeable," "envisioned," "anticipated," or "contemplated."[38]

Not only can the failure to preserve evidence be a crime in and of itself, but it may be used to prove consciousness of guilt for underlying crimes or to enhance criminal penalties.[39] A court may apply sentence enhancements for conduct preceding the start of a government investigation "if the conduct was purposefully calculated, and likely, to thwart the investigation or prosecution of the offense of conviction."[40]

In civil litigation, the failure to preserve evidence can impair the defense. Potential penalties for preservation failures hinge on the degree of culpability and can include monetary sanctions,[41] preclusion of defenses,[42] adverse inferences,[43] and even default judgments in extreme cases.[44]

2. Best Practices For Document And Data Preservation

A company should preserve all information that it knows, or reasonably should know, is relevant to the matter being investigated.[45] When there is doubt, err on the side of preservation, particularly given the possibility that the investigation scope may broaden as additional facts

become known. Counsel should think like an adversary—companies have been punished for ignoring "the possibility that others might have entertained different theories [about which evidence] might have been relevant."[46]

To meet preservation obligations, counsel will first need to take affirmative steps to plan, implement, and monitor compliance within the organization.[47] First, identify the custodians whose documents must be preserved. These are typically the individuals likely to have information about the subject of the investigation.[48] Some will be obvious based on the nature and subject matter of the investigation. Use organizational charts and human resource records to identify additional custodians. Individuals who report to identified custodians, as well as administrative assistants or other support staff, should be considered for purposes of preservation. Do not overlook third parties, including consultants, advisors, and independent contractors whose documents may be considered to be within the company's possession, custody, or control.[49] Expect the list to expand as the investigation unfolds and pay close attention during interviews for new names.

Second, determine where the relevant evidence is maintained. Get a general sense of where the relevant hard-copy documents are stored, and do not forget to look in high-density storage areas and to check with the company's off-site storage vendors, such as Iron Mountain. It is generally good practice to send such vendors a written notice to suspend their document destruction obligations (often set out in a contract) and to request an index of material in storage.

Counsel should speak with IT personnel to understand how electronic information is stored. Electronically Stored information ("ESI") includes

- E-mails and other electronic communications (e.g., instant messages, voicemail, and chat records);
- Documents maintained in document-management systems, shared drives, or network drives; and
- Information in databases and on back-up tapes.[50]

Relevant ESI may be found on laptops, handheld devices, and other similar technologies. IT personnel can provide information about the company's systems, as well as the systems and applications used by key custodians.[51] Someone in the legal department should be familiar with their company's IT systems, retention policies, back-up practices, and IT personnel even before an investigation is contemplated.[52]

Third, suspend all document retention and destruction policies, including any auto-delete features, at least as to relevant custodians or departments. Preserve electronic back-ups likely to include relevant data or documents.[53] This often requires locating and securing physical media.

Fourth, determine the best means of notifying relevant custodians of their document preservation obligations. Usually, it is best to send a "hold notice" to custodians immediately after the nature and scope of the investigation are understood and after the key players and systems are identified. A hold notice should be written in plain English (or in the language spoken where potential custodians reside). An example of a hold notice is included in Appendix A. At a minimum, a hold notice should:

- Summarize the subject matter of the investigation, including the relevant time period covered by the investigation.
- Instruct custodians to preserve all documents potentially relevant to the subject matter and inform them that all regular document retention and destruction policies are suspended until further notice.
- Inform custodians of the definition of document or communication so that custodians understand the breadth of the preservation obligation.[54]
- Provide a numbered list of relevant documents that must be preserved.
- Inform custodians of the importance of preserving and warn them of the potential risks and severe consequences of not preserving documents.
- Provide contact information for counsel who can answer any questions about the preservation obligation.

In many cases, it is prudent to require the recipients of the hold notice to acknowledge receipt and understanding of their obligations. The investigators may even wish to conduct a preservation interview with custodians to ensure they understand their preservation obligations and to determine where relevant documents are maintained. One way or the other, counsel will need to verify compliance. Otherwise, counsel may be creating a bad record that can be used later by adversaries to challenge the adequacy of the preservation efforts.[55]

While hold notices are typically distributed broadly and simultaneously to all key players, the timing of the hold notice may be calibrated to permit preservation efforts before a targeted employee has the opportunity to destroy evidence. This may include imaging hard drives and instituting ongoing monitoring of employees' e-mail accounts and other ESI.[56]

Finally, preservation efforts should be carefully documented. Create a log or a memo to file documenting each step of the process. Some of the key data points to record include:

- The names of the key custodians;
- The date on and means by which they were identified as custodians;
- The date they received a hold notice;
- The date(s) that they acknowledged their preservation obligations;
- The types of ESI preserved;
- The dates when each custodian's ESI was captured; and
- Any problems that arise and the resolution of those issues.

As discussed below, third parties such as auditors and the government will be keenly interested in a company's preservation efforts. So while a memo should be maintained by an attorney (or someone working at the attorney's direction) to maximize potential work-product protection of the record, counsel may later find it necessary to share this with the government or litigation adversaries.

B. Document Collection

After the investigators take steps to preserve documents, they will need to collect documents for review and analysis. They will most likely collect only a subset of the documents designated for preservation. The protocol for hard copy and electronic document collections may differ, but the key to both collections will be to plan them in advance and document how they were carried out.

1. Protocol For Hard Copy Document Collection

The first decision to make is who should collect the documents. To avoid later questions about the integrity and thoroughness of the process, do not simply ask employees to choose relevant documents to forward to someone's attention. It is important for an attorney to supervise and actively participate in the collection process. Paralegals and administrative staff can help. An attorney, however, should ensure that the correct judgment calls are made about what to collect, how to collect, and how to document the effort.

When possible, an in-person interview should be done as part of the collection. (If not done already, this interview also presents an opportunity to review with the employee her preservation obligations.) The interview should take place either in the employee's workspace or a nearby location, so that the interviewers can collect the hard copy documents during or immediately after the meeting.

Use a document interview questionnaire with a uniform set of questions. (An example of a document interview questionnaire is included in Appendix B.) At the top of the questionnaire, record who is conducting the interview, the date and location of the interview, the name of the witness, and the name of the matter for which the documents are being held. While most companies will have official policies on document retention, each employee should be asked about her personal practices for document creation, retention, and destruction.

With respect to hard copy documents, questions should elicit all locations where the employee might store documents, including locations away from the office (such as in a home office), or in other company locations (such as with an administrative assistant, colleague, or in hallway or off-site storage). Identify the types of relevant hard copy documents the custodian keeps, such as hard copy reports the employee regularly receives, calendars, notebooks, or a phone log. Everyone with a role in the collection should use the same format for recording this type of information. Maintain a central repository for the questionnaires and any other documents that the team creates to memorialize the collection.

The scope of the actual collection will, of course, depend on the scope of the investigation and the employee's role. But keep in mind that re-collecting from individuals or locations that already have been searched should be avoided if possible. And an accurate record of what was collected and from where will save time down the road if another collection becomes necessary.

After documents have been collected, the investigators may decide to make copies and return the originals. Or, they may retain the original documents if the documents are not currently in use or if there is any concern about their destruction or alteration.

2. Protocols For Collection Of Electronically Stored Information

The collection of electronic stored information ("ESI") can be complicated and expensive. In-house IT personnel are a good place for information about the location and format of ESI, but unless the staff has previously performed forensic collections, look for outside expertise.

How to choose a vendor? In addition to cost (which can vary significantly), research the vendor's experience and reputation, the methods and imaging software that they use, the vendor's geographical reach (whether they can seamlessly collect documents in all of the company's offices, even overseas), and the vendor's availability (whether they can send someone to the field tomorrow).

There are two important considerations that apply to the collection of ESI — preservation of metadata and documenting the "chain of custody."

Metadata is "'data about data' or the information underlying information."[57] This data is usually not apparent on the face of the document, but provides a wealth of information, such as where the document was stored, who had permission to access it, and when was it created, edited, or forwarded.[58] The production of metadata has become routine.[59] The improper collection of ESI (e.g., using a "drag and drop" method) may result in alteration of the metadata, including the file's "date modified." Experienced collection vendors will have the necessary tools for properly "imaging" the ESI in a forensically sound manner that will not change the metadata and will satisfy government agencies, and the courts, should the data ever have to be produced.

Chain of custody is particularly sensitive with ESI because of the ease with which electronic data can be altered. Should data be produced to a regulator or litigation adversary, the company may be required to submit declarations attesting to the collection process, including who had access to the collected information and how it was collected. Vendors that specialize in collecting ESI have set protocols to establish chain of custody and should be willing to provide declarations, or even court testimony, if necessary. When hiring a vendor, ask for information about their chain of custody provisions and their willingness to provide testimony. Having a third-party vendor responsible for ESI will lessen the chance that an attorney will have to become a witness to discuss document collection efforts.

In determining what ESI to collect, the same considerations apply as in determining what hard copy documents to collect. If hard documents are collected from an individual, that individual's ESI should be collected as well. And, importantly, use the same document questionnaire for the hard copy and ESI collections. Ask about the types of ESI the person keeps, where it is located, and how to access it. Share examples of places where ESI might be maintained, such as hard drive- and network-based e-mail, "shared" drives (*i.e.*, drives where multiple people store their work), instant messages, and personal devices connected to the company's network. Collect passwords or similar credentials to access protected information.

The vendor may be able to collect and copy some ESI remotely, with the assistance of the company's in-house information technology staff. In many instances, however, it will be necessary to have the vendor on-site at the time of the witness interviews so that forensic images of the employee's computer and other electronic devices can be made at the same time hard copy documents are collected.

C. Data Management, Processing, And Review

Once documents are being collected, the investigators will need a place to store, organize, and review them. The tools selected will largely depend on the amount of information collected. Remember, these tools will be used throughout the investigation, as well as through any post-investigation regulatory action or litigation, so the options should be carefully considered.

The investigation team first needs to determine how the information should be managed. Hard copy documents can either be reviewed in print or electronically. If the collection results in just one or two boxes of documents for review, it may be manageable to make copies of the documents, review them on paper, and flag relevant pages. However, if there are dozens of boxes of documents, it may be more cost-effective to have the documents scanned for electronic review on a database. Reviewing documents on a database allows the reviewer to "tag" documents electronically for issues and relevancy. Furthermore, because the text of documents scanned for a database is usually processed via optical character recognition ("OCR"), reviewers can search the text and organize the documents.

There are also different means of managing ESI depending on the volume of data, time constraints, and costs. Many law firms and some companies are equipped with in-house review tools and the technical staff necessary to manage small volumes of documents. However, if there is a large amount of data, the resources of a third-party vendor may be required.

Once a data host has been selected, the data must be processed. This means narrowing the documents for review using key terms, date ranges, and other criteria. Brainstorm terms likely to appear in relevant documents and ask the vendor to apply them to the database. The resulting "hit list" will show how many documents contained each search term. Analyze the hit list to identify "false positives" (*i.e.*, terms yielding many documents with no relevance) and refine or eliminate those terms. Occasionally, key words will need to be added as the investigation proceeds. Keep a careful record of the searches run and the hits for those searches.

After the search terms have been finalized and a set of potentially relevant documents identified, the review can begin. Before starting, the investigation team should develop and reduce to writing a review protocol. This will be a system of "tags" or "codes" used to flag documents as relevant to particular issues under investigation. Particularly important documents may be tagged "of interest." (More colorful designations such as "hot" or "key" are generally not helpful.)

After the first-level reviewers have flagged all the potentially relevant documents, more senior attorneys will be tasked with conducting a second level review for quality control. These attorneys may also develop ways to make the review more efficient, for instance, by identifying irrelevant documents that can be tagged accordingly in bulk. The document reviewers should always have a point person, or persons, to contact with technical and substantive questions.

As technology advances, so will methods of review. For example, in a typical document review, each document that makes it through the initial search filters (i.e., that are responsive to a list of search terms or that fall within a certain date range) is reviewed by an attorney. This is obviously time-intensive and thus expensive. As an alternative, some companies have used "computer-assisted review" tools. Generally, such tools require a senior attorney to review and code a "seed" set of documents. This coding is fed into predictive software that analyzes the data and develops search criteria to help determine, without manual review, the relevance of the larger universe of

documents.[60] Although the adequacy of such methods have received very little scrutiny by the courts, in February 2012, United States Magistrate Judge Andrew Peck, of the Southern District of New York, issued the first court order approving the use of this type of automated review in litigation.[61]

V. Conducting Interviews

Interviews form an integral part of almost any investigation work plan. This section discusses how to best assure that interviews are protected as privileged communications and conducted in an ethical manner. It also addresses how to prepare for and conduct interviews, including some commonly encountered hazards, and the considerations in determining how to memorialize the interviews.

A. Privilege And Ethical Considerations

1. Is The Interview Privileged?

Whether the attorney conducting the investigation is an in-house lawyer or from a firm working on behalf of a Board committee, one thing is clear: She should not also represent witnesses. The question arises then: Is counsel's interview of the witness protected from later disclosure by the company's attorney-client privilege? The answer may depend on whether the interviewee is, at the time of the interview, a current employee, a former employee, or unaffiliated with the company.

In *Upjohn Co. v. United States*,[62] the Supreme Court held that the attorney-client privilege applies to communications between an employee and corporate counsel where:

- The communication is made at the direction of corporate superiors;
- To secure legal advice for the corporation;
- Concerning matters within the scope of the employee's duties; and
- The employee knows that he is being interviewed so that the company can obtain legal advice.

Assuming these four conditions are met, an investigative interview should be privileged.[63]

Upjohn did not address whether the privilege protects communications with former employees. Other courts, however, have extended the privilege where they relate to communications with counsel before the employee separated from the company. Communications with a former employee may also be privileged if the communications concern actions that the employee took, or knowledge that the employee obtained, during his employment. However, an interview with a former employee relating to facts developed after the employee left generally will not be privileged.

Communications with third parties who were never employees of the company are usually not privileged. The work-product doctrine may protect information obtained from interviews with third parties (as well as interviews with current and former employees). But work-product protection, even if it applies, is not absolute and does not prevent a third party from disclosing the substance of his communications with company counsel if later questioned. Moreover, unlike the privilege, the federal work-product doctrine applies only to materials prepared in anticipation of litigation. Accordingly, interview third parties only where there is a compelling need to do so.

2. Ethical Considerations

An interview of an employee witness also gives rise to certain ethical considerations. The ABA Model Rules for Professional Conduct, for example, bar attorneys from providing legal advice to an unrepresented person if they know or reasonably should know that the interests of that person are or have a reasonable possibility of being in conflict with the interests of the client.[64] The Rules also require counsel to identify her client where she (1) is communicating with an organization's directors, officers, employees, or other constituents and (2) knows or should know that the organization's interests are adverse to the witness's.[65]

Adversity between an interview witness and counsel's organizational client is not uncommon. Not only can an investigation result in discipline for the witness, but companies sometimes decide to share facts harmful to a witness (including the substance of the interview) with the government. It is therefore important for the witness to understand who the lawyer does (and does not) represent and for counsel to avoid saying anything that could be construed as legal advice.

Any misunderstanding on these points can lead to the inadvertent formation of an attorney-client relationship with the witness. Under the Model Rules, an attorney-client relationship may be formed where the potential client manifests intent for the lawyer to provide legal services and the lawyer manifests consent to do so. A lawyer obtaining confidential information and rendering advice is deemed to assent to representation.[66]

An attorney-client relationship with a witness could force counsel to withdraw if the "client-witness" is responsible for misconduct. Moreover, the witness may claim that his conversation with counsel was privileged, confidential, and inadmissible, hindering the company's ability to discipline the employee limit indemnification and advancement of expenses, or share the substance of the interview with regulators or law enforcement.

3. The *Upjohn* Warning

To prevent an attack on the privilege or counsel's ethics, the lawyer should administer to each witness an "*Upjohn* warning" at the beginning of the interview. Based on the Supreme Court decision described above, an *Upjohn* warning should consist of the following:

- My name is _____. I represent Corporation. I do not represent you.
- I am conducting this interview to collect facts to provide legal advice to Corporation.
- This interview is part of an investigation to determine the facts and circumstances surrounding _____.

- This conversation is protected by attorney-client privilege. But the privilege belongs to Corporation, not you.
- Do not share the substance of this conversation with anyone, including other employees or third parties.
- Corporation, and Corporation alone, may decide to waive the privilege and share the substance of what we discuss here today with third parties, including the government. That decision is within Corporation's sole discretion and will be made without notifying you.
- Do you have any questions? Are you prepared to proceed?

Some practitioners argue that, if the company is likely to share the interview with the government or other third party, counsel should say so as part of the *Upjohn* admonition. But because confidentiality is an element of privilege, a determination to disclose the substance of the interview before conducting the interview would seem to render the interview non-privileged from the beginning. In other words, if counsel conducts the interview with the intent to waive privilege, there is no privilege to waive. Better to wait to make such decisions until the investigation is complete.

The *Upjohn* warning should be memorialized by noting in interview notes or memoranda that the warning was given. For extra assurance, before starting the interview, counsel should ask the witness to sign an acknowledgement that he received and understood the *Upjohn* admonition.

4. Other Admonitions To Witnesses

In addition to the *Upjohn* warning, advise witnesses:

- Not to discuss the interview with anyone else—it is important that each interviewee's recollection be his or her own;
- Not to do independent investigation—if there is a person who might have relevant information, or a document source that could be useful, the witness should tell the investigation team;
- Leave all relevant documents, paper and electronic, exactly as they are (if the witness has any sort of auto-delete settings or shredding schedule, those arrangements should be suspended); and
- Not to prepare a follow-up memo or writing to counsel—if the witness remembers additional information, the witness should arrange a call or meeting with the investigators to present that information.

B. Preparing For The Interview

1. Witness Sequence And Timing

The work plan prepared at the beginning of the investigation will typically include an initial list of witnesses to interview. *See* Section II.D, *supra*. The sequence in which the investigators speak to

these witnesses, however, merits some planning as well. Some practitioners like to start with short interviews of key players, confident that they can "circle back" to those witnesses should lower-level employees spur additional questions. Others prefer to start at the bottom of the organizational pyramid and work their way up to key decision-makers.

Other relevant factors include the progress of the document review. Often, compiling and reviewing relevant documents prior to interviewing witnesses is more efficient in the long term, even though it may delay speaking to those privy to the facts. Or, it may be more effective to "strike while the iron is hot," interviewing witnesses about important events before memories fade.

2. Interview Outline

An outline will help keep the interviews on track and flowing in a logical manner. An outline also helps to ensure that all necessary topics are covered. The outline should be supplemented with a binder of reference materials, such as organization charts, internal policies and procedures, and important rules or regulations (such as any relevant accounting standards).

A list of general topics, such as "process for resolving questions about revenue recognition," as well as specific items to review, such as "memorandum dated X regarding Acme revenue recognition," can often be sufficient, as opposed to a list of scripted questions. As when conducting a deposition, an interviewer should not be too wedded to the sequence of her outline. Instead, listen to the witness, who may raise interesting and relevant points not previously considered. Follow up and always give the witnesses ample opportunity to explain and amplify.

3. Documents

Although the effective use of documents is key in any interview, there is no one "correct" technique. The interviewer may present a document, ask about it, and then broaden the discussion to related topics. If the witness's statements are not controversial or inconsistent with the document, a detailed review of the document may be unnecessary. Or, the witness may be asked about a topic without documents. This is often an effective way to exhaust the witness's memory on an issue without limiting the discussion to the specifics of the document.

A witness or his counsel may ask for copies of the documents to be used in the interview in advance. Some practitioners decline to do so, fearing that sensitive company documents could be distributed more broadly, that any work-product protection attaching to the compilation will be lost, and that counsel will lose the opportunity to gauge the witness's unrehearsed response to the documents. Other practitioners believe that the risk the documents will be abused by reputable counsel is minimal, the work-product value of such compilations is small, and the considered response of witnesses to previously reviewed documents is likely to be more accurate and reliable.

C. Common Issues

1. Who Should Participate?

Keeping the interview confidential and each witness's recollection untainted by the views of others are important aspects of any investigation. Accordingly, only the witness and his counsel (or, where required, union representative) should attend each interview. Decline requests for "group interviews" conducted "for the sake of efficiency," or for witnesses to be accompanied by subordinates "closer to the facts."

Remember, being interviewed can be a stressful, uncomfortable, and intimidating process. And the *Upjohn* warning will do nothing to relieve any witness anxiety. Be mindful of these concerns and pick a private, well-lit interview site. Offer the witness reasonable breaks as needed, be respectful of the witness's time, and discuss their scheduling constraints well in advance.

2. Witness Refuses To Cooperate

Sometimes a witness will decline to cooperate. The possible reasons are manifold and sometimes quite innocent. The witness may not understand the purpose of the investigation or that it is being conducted on the company's behalf. Alternatively, the witness may have something to hide or someone to protect. If the refusal is not simply a case of confusion, review the organization's code of ethics, relevant employment agreements, collective bargaining agreements, and state employment law. In most cases, an employer has the right to require the employee's cooperation. As a result, the company may inform the witness that that if he does not cooperate, he will face disciplinary action.

A witness may be reluctant to answer questions out of fear of retaliation. No one should promise anonymity or anything else in exchange for cooperation. The witness can be reminded of any company policies that require his participation. But for the reasons discussed above, the investigators should not offer an assessment of the witness's legal exposure, a description of applicable "whistleblower" protections, or anything else resembling legal advice.

3. Witness Requests Counsel

Although in most cases employees do not have a legal right to counsel when responding to questions from their employer, if an employee requests a lawyer, consider permitting it, even if that means suspending an ongoing interview. Allowing a witness to have counsel is often fair, particularly if the witness is facing civil or criminal sanction. And a represented witness can be a more focused and productive. If a witness is properly prepared, he may enter the interview with his memory refreshed, mindful of the importance of candor.

An employee may request that the company pay his legal fees in connection with an internal investigation. For a discussion of the issues surrounding indemnification and advancement of fees, see Section VIII, *infra*.

D. Memorializing The Interview

Where possible, another attorney or a paralegal should attend. By having a second person attend, the interview will likely be more efficient, the record of the interview more comprehensive and accurate, and the risk of missing or forgetting an issue minimized.

In most cases, witness interviews should be memorialized in the form of detailed notes or interview memoranda. By doing so, the issues reviewed, lines of inquiry, and information provided by each witness will be recalled, not only in the near term, but weeks, months or even years down the road. However, carefully consider all decisions regarding how to memorialize witness interviews, given the possibility that interview materials ultimately may be subject to disclosure to the government or an adversary.

The most common manner of documenting an interview in writing is with attorney notes prepared during the interview. Ideally, if counsel chooses to use interview notes, an attorney other than the interviewing attorney should serve as note taker. Notes should be thorough and accurate.

In many instances, counsel may choose to supplement notes with an interview memorandum, which should be prepared as soon after an interview as possible to ensure accuracy. A memorandum may be useful if the investigation is likely to be complicated or last more than a few weeks, if investigators who did not participate in an interview wish to review a summary of the interview, or if the interview is conducted in another language.

If detailed notes or interview memoranda are prepared, the following steps should be taken to protect these documents as being privileged and attorney work-product:

- Do not simply recite facts. Notes and memoranda should include the attorney's thoughts and mental impressions. Avoid attempting to capture direct quotations from witnesses, and intertwine any factual details from an interview with thoughts and mental impressions. In memoranda, avoid using a "Factual Background" section. Lastly, avoid memorializing legal conclusions.
- As noted above, memorialize the *Upjohn* warning. Putting the *Upjohn* warning in writing reinforces that the interview was for a legal purpose, not a business one. It also protects an attorney against a witness's claim that the witness formed an attorney-client relationship with the attorney.
- Memorialize document-retention instructions. Notes and memoranda should reflect that such instructions were given and also that the witness confirmed understanding the instructions.
- Mark the document as protected. Insert words such as "Privileged and Confidential – Attorney Work-Product" at the top or bottom of each page.
- Store the document securely and limit access to it.

Never give written notes and memoranda to a witness (or his counsel). Avoid recording an interview in any form (e.g. audio, video, written transcript), as recordings are less likely to be protected as attorney work-product. Avoid making flippant, extraneous comments in notes and memoranda, such as stating that a witness is "corrupt" or a "liar."

Finally, the memorialization of the interview should include a careful record of all documents shown to the witness. For each interview, keep a separate copy set of the documents reviewed.

VI. Special Issues In Cross-Border Investigations

When the scope of an internal investigation requires inquiry into issues outside the United States, special—and often tricky—issues arise. Chief among these are differing rules governing the attorney-client privilege in foreign jurisdictions, foreign data privacy laws, and various requirements and limitations imposed by foreign labor and employment laws. Consider these in consultation with local counsel when planning and executing a cross-border internal investigation.

A. Attorney-Client Privilege

1. Recognition Of Attorney-Client Privilege

The U.S. Supreme Court has heralded the "attorney-client privilege [a]s the oldest of the privileges for confidential communications known to the common law."[67] Unsurprisingly, then, courts in common law jurisdictions around the world generally recognize *some* form of privilege that attaches to confidential communications with attorneys.[68] The same is true for many civil law countries, such as France and Germany—although the concept tends to be less developed given the absence of adversarial discovery procedures in the legal system.[69]

While there may be overarching similarities governing privilege issues, there can be significant variations from country to country. For example, as discussed below, even where a jurisdiction recognizes the concept of attorney-client privilege, the privilege may not extend to in-house counsel or to others working at the direction of counsel, as it can in the United States. And even in jurisdictions that nominally recognize the privilege, it may in practice be interpreted very narrowly or not applied at all. In China, for instance, the Lawyer's Law Article 38 imposes a duty on attorneys to maintain confidential information if requested by the client; in practice, however, attorneys generally can be compelled to divulge such communications in court proceedings.[70]

Given the differing rules and practices concerning attorney-client privilege in various jurisdictions, any cross-border internal investigation should begin with an evaluation of the governing ground rules for privilege.

Nor should one assume that a U.S. court or regulator will honor U.S. privilege law for information learned abroad. Most U.S. courts apply a "touch base" analysis to determine whether U.S. or foreign privilege rules will apply.[71] This involves a fact-intensive analysis, focused on whether the communications "have a 'more than incidental' connection with the United States."[72] Given the nuances of that analysis, investigators should honor (to the extent possible) foreign privilege laws in conducting a cross-border investigation.

2. Applicability Of Privilege To In-House Counsel

In the United States, it is clear that the attorney-client privilege attaches to in-house counsel acting in the capacity of a lawyer, *i.e.*, when the relevant communication is made in confidence for the purpose of seeking or rendering legal advice.[73] That it *not* the case, however, in many foreign jurisdictions, where in-house attorneys may not be considered sufficiently "independent" to justify application of the privilege or may not be members of a bar.[74]

For example, the Court of Justice of the European Union ("EU") recently considered whether communications during an investigation from an in-house lawyer of an English company to the company's Director General were privileged.[75] The court, upholding longstanding European precedent, held that because of "the in-house lawyer's dependence and the close ties with his employer, he does not enjoy a level of professional independence" necessary for the privilege to attach.[76] Although this ruling was under EU law, similar restrictions on the ability to claim privilege over communications with in-house counsel exist under the law of various European Union member states.[77] The ability to claim privilege over communications with in-house counsel in jurisdictions outside of Europe also varies widely.

Given the variety of approaches to this issue, an organization may need to rely on outside counsel if it seeks to protect the attorney-client privilege.

B. Foreign Data Privacy Laws

1. Data Privacy Overview

Approximately 70 countries have some type of law that regulates the collection, use, and disclosure of personal information. Whereas the United States has a myriad of federal and state privacy laws protecting certain types of information (such as financial and health information) or certain groups deemed more vulnerable (such as children), Europe and other foreign jurisdictions have adopted omnibus privacy legislation regulating the collection and use of all personal information across all sectors of the economy.[78] These laws can cover public and private sector collection, use and disclosure of personal information, as well as its transfer across national borders.

These omnibus privacy laws usually require that individuals whose personal information is collected be given notice of, and in certain circumstances consent to, the collection, use and transfer ("processing") of their personal information. Accordingly, individuals have the right to know what information about them is collected, how it is used, and with whom it is shared. In addition, such collection, use and disclosure must generally be registered with an independent data protection authority ("DPA"), and in some countries, the DPA must consent to the exporting of personal information to another country. DPAs may refuse permission to export if the data protection laws of the receiving country are not considered to be as strong as those of the home country or if the DPA believes that the contemplated uses of the personal information are excessive.

Security of the personal information is also very important. In some countries there are very detailed and particular technical and organizational security measures that must be implemented.[79]

a) Europe

The Directive of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the movement of such data (95/46/EC) (the "Directive")[80] establishes strict requirements for the processing of personal data within the EU and the transfer of personal data outside the European Economic Area ("EEA").[81] Although the Directive harmonizes the laws in EU Member States[82] to some extent, details of data protection regulation in the EU remain governed by the particular laws of the Member States.

The Directive applies to all "processing" of personal data. "Processing" is defined to include the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction of data.[83] "Personal data" means data which relates to an identified or identifiable individual (*i.e.*, someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity).[84] That means information such as business contact information is considered personal data.

Under the Directive, four relevant obligations must be satisfied:

1) Individuals must be provided with notice;

    - In general, an individual from whom personal data is collected must be informed about: (a) what personal data are collected; (b) the purpose(s) for which the personal data are intended to be processed; (c) to whom the personal data will be disclosed; and (d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data to be fair.[85]

2) The purpose(s) for which personal data are used must be related to the notice provided;

    - The personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.

3) There must be a legal basis or "good reason" for each act of processing; and

    - All processing of personal data requires a legal basis.[86] The possible legal bases for processing personal data include: (a) the individual has unambiguously given his consent; (b) the processing is necessary for compliance with a legal obligation to which the data controller is subject; and (c) the processing is necessary for the purposes of a legitimate interest, except where such interest is overridden by an individual's protected fundamental right or freedom.

4) The personal data must only be disclosed to organizations that will adequately protect the data.[87]

    - Generally speaking, transferring data outside of the EEA is not permitted. The exception to that rule is that personal data may be transferred to an organization that has been determined to provide "adequate" protection to personal data.[88]

Failure to comply with EU Member State privacy laws can affect organizations with operations in the EU in a variety of ways, *e.g.*,:

- EU privacy regulators may suspend or block transfers of information from EU subsidiaries or branch offices;
- Privacy regulators and law enforcement agencies may impose administrative, civil, and criminal penalties;
- Individuals generally have a private right of action to recover damages arising from violations of their privacy rights;
- There may be a loss of reputation, employee morale, and goodwill.

b) Asia-Pacific

The data privacy laws in Asia-Pacific vary widely from country to country, particularly with respect to the processing of employee data and cross-border transfers. For example, Australia's legislation exempts much employee data, whereas the legislation in Taiwan, Hong Kong, and Japan covers employee data. Australia also restricts cross-border data transfers by organizations to recipients in foreign countries that are subject to a "substantially similar" privacy regime, whereas the law in Japan applies the same rules to all third parties regardless of their location. However, all of these laws have the following requirements:

- Individuals must receive notice about what personal information is being collected, the purposes for which it will be used, and the types of third parties with whom the personal information will be shared;
- Individuals must be given choices and means to limit the use and disclosure of their personal information; and
- Personal information must be protected from loss and misuse, and unauthorized access, disclosure, alteration, and destruction.

c) North And South America (Other Than The United States)

The data privacy laws in North and South America also vary widely from country to country. Of all the countries in Latin America, Argentina has the most developed framework for the protection of personal information. It enacted a comprehensive, EU-style data protection law in 2000 and also provides individuals with a constitutional right to obtain information on the data held in files or databases.

In Canada, private sector use of personal information is regulated at the federal level and that legislation also applies to all businesses and organizations that collect, use, or disclose personal information where "substantially similar" provincial legislation does not apply. Currently, privacy legislation in the provinces of Alberta, British Columbia, and Quebec has been deemed substantially similar. The Canadian federal legislation applies only to personal information for organizations that are regulated within the legislative authority of the Parliament of Canada.[89] Unlike other privacy laws, such as the EU Member State laws, personal information does not currently include the name, business title, business address, or business telephone of an employee of an organization *(i.e.*, information on a business card) and the federal legislation does not explicitly restrict cross-border transfers.

2. Protocols For Collection And Review

a) Notice

In most, if not all, of the jurisdictions discussed above, notice must be given to those employees whose personal data will be processed (*i.e.*, collected, reviewed, disclosed and transferred) as part of an investigation. Notice may be provided in a variety of forms, *e.g.*, stand-alone notices, employment contracts, employee handbooks, or document retention/collection notices. Accordingly, new notice may not be required if sufficient notice has already been given. However, if the existing notice is insufficient in any respect, new notice should be provided. The form of the notice is not important; what is important is that the notice constitutes sufficient and complete notice of the personal data collection, review, disclosure, and transfer.

Be broad and explicit when giving employees notice of the purposes to which the information will be put so that the company's ability later to process the data will not be unduly restricted. For example, if data will be provided to the SEC, inform employees that the data will be shared with U.S. law enforcement and regulatory agencies. That way, data can be provided in response to a later request from DOJ without new notice.

b) Legal Basis

In those jurisdictions which require an articulated legal basis for processing data, the organization may be able to rely on the following possible legal or "good reasons" to process the data:

- It is necessary for compliance with a legal obligation;
- It is necessary for the purposes of a legitimate interest; or
- The individuals have given unambiguous consent.

"Necessary to comply with a legal obligation" is interpreted fairly narrowly. For example, in some jurisdictions the legal obligation must be imposed on the entity in that jurisdiction, and not on the entity that is investigating, or any other affiliated entity. Moreover, it will be more difficult to rely on this legal basis in the context of an internal investigation, rather than an external regulatory one, such as responding to a subpoena from the DOJ or SEC.

The "balance of interest" basis will be available in many jurisdictions. For example, in the UK the DPA has confirmed that it takes a wide view of the legitimate interests condition and recommends that two tests be applied to establish whether this condition is met: The first is the legitimacy of the interests, and the second is whether the processing imposes unwarranted prejudice to the rights and freedoms or legitimate interests of the individual.

The existence or validity of consent will be assessed in the light of all of the facts. In the EU, the Directive defines consent as "any freely given specific and informed indication of his wishes by which the [individual] signifies his agreement to personal data relating to him being processed." The fact that the individual must "signify" his agreement means that there must be some active communication between the parties. Although an individual may "signify" agreement other than in writing, the lack of a response to a request cannot be interpreted as consent. Moreover, to be deemed valid, consent must be fully informed. Thus, consent obtained on the basis of misleading or incomplete information will not be valid.

3. Data Export Restrictions

If the investigation is being conducted in the EU, personal data may be transferred if:

- The entity that receives the information is in the United States, and that entity has certified its compliance to the EU/U.S. Safe Harbor Framework (the United States itself is deemed not to provide an adequate level of protection);
- The individual has unambiguously given her consent;
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims; or
- The exporting and importing organizations have entered into a contract.[90]

These mechanisms are examined in detail below:

a) Safe Harbor

The Safe Harbor Framework was developed to provide U.S. organizations with a streamlined means of satisfying the "adequacy" requirement under the EU Directive. U.S. organizations that certify to the Safe Harbor are deemed to have adequate protections for personal data.

The Safe Harbor Framework consists of seven Safe Harbor Principles, 15 frequently asked questions and answers, the European Commission's ("EC") adequacy decision, the exchange of letters between the DOC and the EC, and letters from the Department of Transportation ("DOT") and Federal Trade Commission ("FTC") on their enforcement powers. For a U.S. organization to be eligible for the Safe Harbor, it must be subject to the jurisdiction of a "government body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices . . . in case of noncompliance with the [Safe Harbor] Principles."[91] To comply with the Safe Harbor, organizations must undertake specific actions with respect to the personal data received from the EU. These actions include:

- Providing notice to individuals when the personal information transferred to the organization is used for a different purpose or disclosed to a third party;
- Providing individuals with the opportunity to opt out of third-party disclosures or uses that are incompatible with the purpose(s) for which their personal information was originally collected; or in the case of sensitive data, obtaining opt-in consent to use the data for a different purpose or disclose it to third parties;
- Executing onward transfer agreements (to govern transfers to third parties);
- Providing individuals with access to relevant information;
- Implementing security measures to protect the data;
- Ensuring data integrity (i.e., reliable for intended use and accurate, complete, and current); and
- Establishing enforcement mechanisms.

b) Consent

Depending on the nature of the investigation, consent may or may not be an available option for validating cross-border transfers. Consent is "any freely given specific and informed indication of his wishes by which the [individual] signifies his agreement to personal data relating to him being processed." Moreover, consent must be a fully informed.

c) Establishment, Safeguarding Or Defense Of Legal Claims

Another way to establish adequacy is to establish that the transfer is necessary or legally required for the establishment, safeguarding or defense of legal claims. At first glance, this might seem like a promising avenue in the context of an investigation.

But, the Article 29 Working Party, an independent EU advisory body on data protection and privacy, has stated that the concept of establishment, safeguarding or defense of legal claims "cannot be used to justify the transfer of all the employee files to [a multinational] group's parent company on the grounds of the possibility that [legal proceedings by an employee of the group currently posted to an EU subsidiary] might be brought one day."[92]

The Article 29 Working Party's guidance is not binding on the individual DPAs but it does present a majority view of the data protection commissioners in the EU. The UK's DPA has not followed this very strict interpretation, however, and has stated that the UK's derogation regarding legal claims applies for the purpose of, or in connection with, any legal proceedings,[93] including legal proceedings outside the UK and prospective legal proceedings.[94] There is still, however, a question as to whether an internal investigation would be sufficient to qualify as a legal proceeding or a prospective legal proceeding under the UK Information Commissioner's interpretation.

Even if the concept of the establishment, safeguarding or defense of legal claims is available as a basis for transfer, the Article 29 Working Party has confirmed[95] that it can be applied only if the applicable international rules governing criminal or civil proceedings have been complied with, notably as they derive from the provisions of the Hague Convention of March 18, 1970 ("Taking of

Evidence Convention")[96] and of October 25, 1980 ("Access to Justice Convention").[97] The United States is not a signatory to the Access to Justice Convention and U.S. law does not require courts to follow the procedures of the Taking of Evidence Convention.

d) Contracts Incorporating The Standard Clauses

The EC has adopted two different sets of Standard Clauses for the transfer of personal data outside the EU.[98] Under both sets, the data exporter and importer agree to process data in accordance with certain standards and confer upon data subjects the right to enforce the contract as third-party beneficiaries. Where personal data are being transferred from an EU subsidiary to a U.S. parent, such transfers may be allowed by an existing contract between the two entities incorporating the Standard Clauses. Any such contract should be carefully reviewed to ensure it properly covers the proposed transfer.

C. Labor And Employment Law Considerations

In the United States, where employment typically is "at will," the common practice is to require employees to participate in an investigation or be subject to discipline, including termination. Things are not so straightforward in most foreign jurisdictions. Labor, employment, and (as noted above) privacy laws of many countries offer broad protection to employees.

For example, foreign jurisdictions may permit an employee to refuse an interview by company counsel—especially if the employee is under investigation—or even to refuse to provide evidence against co-workers. In certain jurisdictions, the employee may have a right to counsel or an employee representative at the interview. Moreover, local laws and regulations may limit or prohibit discipline of an employee who simply refuses to cooperate.

Local labor law issues can become even thornier when considering discipline for wrongdoing at the investigation's conclusion. The possible factors are too numerous to mention here, but they can include whether the employees works for a U.S. or foreign entity, whether the conduct in question was prohibited by company policy, whether that policy was established in accordance with local law (in China, for example, proposed workplace rules may have to be circulated for comment before adoption), whether the policy was published to the employee, whether the employee received training on the policy, whether the employee received required notice of the violation, whether the employee is subject to a collective bargaining agreement, etc. If discipline for an employee outside the United States is likely, consult with local employment counsel before finalizing the investigation conclusions, as specific factual findings may be required to support employment action.

D. Other Cross-Border Investigation Issues

1. U.S. Jurisdiction Over Foreign Subsidiaries

A U.S. company conducting an investigation involving a foreign subsidiary should weigh the ability of potential adversaries to obtain evidence from that subsidiary. Some companies are

reluctant to transfer documents from a foreign jurisdiction if, by doing so, the documents will be more easily obtained by U.S. regulators or private litigants.

Documents in a foreign jurisdiction may be more susceptible to discovery than commonly believed. For instance, a U.S. parent may be deemed to have "control" over information at a foreign subsidiary, and thus may be compelled by a court or regulator with jurisdiction over the U.S. entity to produce the information.[99] Indeed, courts have compelled U.S. companies to produce information located at foreign affiliates and have sanctioned the failure to do so.[100] In addition, as detailed below, U.S. regulators may be able to invoke the aid of a foreign regulator that has unquestioned jurisdiction over the foreign subsidiary.

2. Dealing With Foreign Regulators

In any cross-border investigation, multiple governments may claim jurisdiction over the subject matter of the inquiry. Therefore, the company should identify each international regulator which may claim an interest in the investigation and to consider how best to address them, if at all. In making this decision, or in responding to queries from an international regulator, counsel should seek counsel from local attorneys familiar with the regulator's expectations and procedures.

In addition, international cooperation among regulators is increasing. Such cooperation may take place formally, pursuant to an international convention (such as the OECD Anti-Bribery Convention),[101] a Mutual Legal Assistance Treaty ("MLAT"), or a Memorandum of Understanding ("MOU") between regulators.[102] In the United States, for example, Congress has expressly authorized the SEC to "provide assistance" to a foreign securities authority investigating laws administered or enforced by that authority—even if the conduct at issue would not constitute a violation of U.S. law.[103] Regulators may also share information and cooperate more informally. High-profile examples of international cooperation include coordinated international inquiries and dawn raids in cartel investigations,[104] and the joint efforts of German and U.S. enforcement agencies in the anticorruption investigation of Siemens AG.[105]

In short, counsel should assume that regulators in each of the jurisdictions where the company operates are in regular communication. For that reason, the decision of whether to self-report a potential violation of law should be informed by the likelihood that what the company communicates to one regulator will be shared with others. Indeed, some foreign regulators have an expectation that they will be notified at the same time that the company chooses to self-report to U.S. regulators. For example, the U.K.'s Serious Fraud Office (SFO) has said that it "would expect to be notified at the same time as the [U.S.] Department of Justice" of a corruption violation if it also fell within the SFO's jurisdiction.[106]

Key privilege considerations may also arise when dealing with foreign regulators—especially where the regulators request or expect to receive investigation results. In some jurisdictions, a client may be able to selectively or partially waive privilege in reporting investigation findings to government authorities, without fear that the disclosure will constitute a "blanket" privilege waive as to all third parties.[107] Other jurisdictions, however—including the United States—frown upon and may not recognize a "selective" waiver of privilege.[108]

VII. Communications With Third Parties

The company may elect (or be obligated) to inform constituencies outside the company about the investigation well before it is complete. These third parties may include auditors, regulators and law enforcement, and shareholders. As discussed below, the timing and substance of these communications will have implications for the company's relationship with these constituencies and its ability to maintain the confidentiality of the information developed during the investigation.

A. Communicating With Auditors

Independent auditors expect to be among the first to be told of an ongoing investigation, particularly where the investigation implicates a company's accounting, controls, or management integrity. In part, that is because the auditor has issued an audit opinion, which has been published to, and relied upon by, the market. In part, that is because, at any given time, an auditor may be planning or executing an audit or review based on assumptions that the investigation may call into question. Apart from an auditor's expectations, if management's failure to share information misleads the auditors, management may be exposed to civil and criminal sanctions.[109]

If the investigation is disclosed to the auditors, the company should be prepared to respond to a broad range of questions and requests. Counsel should describe the team conducting the investigation, their experience conducting similar investigations, and any prior relationship between the company and the investigators. The auditors will likely seek a briefing about the circumstances that gave rise to the investigation and copies of key documents identified so far. The auditors may also request a copy of the investigatory work plan. They will ask about the scope and results of the document collection effort (including specifics about ESI custodians, when the collection occurred, the method by which documents were collected, and the amount of data and documents collected). They may also ask to see the search terms to be applied, a report of the resulting "hits" from the database, and, more often than not, they will suggest additional terms to apply.

Over time, the auditors may seek regular updates from the investigation team. The agenda for such calls and meetings can include progress on the work plan, new issues identified for review, and substantive interview summaries. The investigators may be asked to deliver these updates to accountants from the audit firm who specialize in forensic accounting investigations. It is sometimes said that these forensic accountants perform a "shadow investigation" because they "shadow" the company's investigation.

At the conclusion of the investigation, the auditors will expect a thorough briefing and, perhaps, direct access to documents and witnesses. The implications for such sharing are discussed in Sections IX.B.2 and X.B.2, *infra*.

B. Communicating With Law Enforcement

As discussed in Section II.C.2, *supra*, various federal agencies have adopted policies that, they say, offer lenient treatment to companies that self-report violations of law.[110] Indeed, the SEC

enforcement staff has encouraged companies to report an ongoing investigation as early as possible.

In many cases, self-reporting makes perfect sense. Where counsel knows that the investigation will, ultimately, come to the attention of regulators, the regulators should be notified as soon as practicable. For example, if an investigation calling into question the accuracy of a company's financial statements will not be complete in time to make a required SEC filing, counsel should call the SEC right away. Similarly, if counsel has reason to believe that the whistleblower who triggered the investigation may reach out to the government, counsel should preemptively self-report.

In other circumstances, however, some question the wisdom of self-reporting. Some have argued, for example, that the settlements offered by the government in cases involving self-reported violations of the Foreign Corrupt Practices Act ("FCPA") by low-level personnel are not obviously better than terms offered to companies that do not self-report. Faced with severe sanctions and a low risk of detection, some companies forego self-reporting and choose instead to focus on rigorous remediation. If they are later confronted with a government investigation, they reason, they will still be able to show a thorough investigation and decisive action to fix problems.

Ultimately, the decision to self-report must be determined by the best interests of the corporation. Here are a few factors to consider:

Whether to Self-Report

Pros	Cons
May be required (*e.g.*, broker-dealers, government contractors)	May embroil company in expensive and damaging broader investigation by authorities
Company and individuals may receive "cooperation credit" from regulators and may defer or avoid prosecution	May result in litigation from shareholders and other parties
Simply may be "right thing to do" given egregiousness of conduct	May result in significant legal fees and costs for both company representation and as a result of fee advancement/indemnification obligations
Deterrent impact on future potential wrongdoers	Increase risk of waiver of privileges protecting the internal investigation

Company can avoid surprise, and may have ability to control what information is reported and how it is reported	May create competitive or business partner issues
Through continued cooperation, the company may have better visibility into the regulator's investigation, including timing of public disclosure, sanctions, etc.	Ensuing investigation may not be covered by insurance

If a company decides to self-report, counsel should think hard about which regulator or regulators to inform. Choices include the SEC, the DOJ (and its many divisions, such as the Antitrust Division), the FTC, the Environmental Protection Agency (EPA), and industry-specific regulators, such as the Office of the Comptroller of the Currency. Counsel should consider whether to contact state or local regulators as well.

In many cases, the initial communications about an investigation will resemble those with auditors. Like auditors, regulators and law enforcement will expect to hear about the facts that triggered the investigation and to receive underlying documents. Depending on the circumstances, they may seek assurances about the competence and independence of the investigation team. And they will be acutely interested in preservation of evidence—expect document preservation and collection efforts to be scrutinized.

Satisfied that a credible independent investigation is underway, that evidence is being preserved, and that they will receive a briefing on the investigators' findings at investigation's end, regulators will often forego subpoenas while the investigation continues. Instead, expect to give regular, substantive updates about developments that expand the investigation's scope or procedures. Resist the temptation to provide analytical "reports from the battlefield" while the investigation is in process. The investigator's understanding of the facts may change, and it is frustrating for everyone to have updates turn into a series of clarifications and corrections.

At the conclusion of the investigation, the government will expect a full briefing about the investigation process, findings, and (where necessary) remediation plan. These communications and the privilege implications are discussed in Sections IX.B.2 and X.B.1, *infra*.

C. Market Disclosure

An organization conducting an internal investigation should also consider whether to disclose the investigation to the public. Certain events may trigger an obligation to disclose, such as if the company determines that it cannot rely on previously issued financial statements,[111] if the investigation ripens to a "material pending legal proceeding,"[112] if such a proceeding is "known to be contemplated" by a governmental authority,[113] or if a company's director is a defendant in a pending criminal proceeding.[114]

Aside from those specific instances, however, analysis of whether (and to what extent) to disclose an internal investigation tends to focus on Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5.[115] Among other things, Rule 10b-5 makes it:

> unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, . . . (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, . . . in connection with the purchase or sale of any security.

The question, then, is as broad as whether there is "a substantial likelihood that" the internal investigation will be "viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[116] (In addition to the general statutory and regulatory requirements calling for disclosure of material events, both the NYSE and NASDAQ have rules calling for the disclosure of material news.[117])

This is a broad, open-ended inquiry—one that calls for the balancing of competing interests and is perhaps best made with the input of the company's securities and litigation counsel. Some of the issues to be considered as part of this inquiry are:

- How likely is a legal proceeding to arise out of the investigation?
- Of what magnitude would any resulting legal proceeding be?
- Is the company preparing to make any periodic public statements or filings that might be viewed as misleading in light of the investigation?
- Do any past statements need to be corrected as a result of the investigation findings?
- Is the disclosure more likely to create an unwarranted concern about the integrity or value of the company than it is to correct any prior disclosures the company has made?
- In light of the investigation, can the executives certify the quality of internal controls, in compliance with Sarbanes Oxley Section 404?

Depending on the answers to these questions, the company may need to disclose information concerning its investigation in its filings and evaluate whether any past statements should be corrected.

D. Communicating With Exchanges

If a company's securities trade on an exchange, it should consider whether it is required to inform the exchange's listing or enforcement staff about the investigation. This typically arises when, in violation of the exchange requirements for continued listing, the company cannot timely submit a required SEC filing due to information learned in the investigation.

Under these circumstances, Rule 12b-25 requires the company "no later than one business day after the due date for such report" to file a Form 12b25[118] with the SEC "which shall contain disclosure of its inability to file the report timely and the reasons therefor in reasonable detail."[119] Form 12b25 requires the company to state whether it is "anticipated that any significant change in

results of operations from the corresponding period for the last fiscal year will be reflected by the earnings statements to be included in the subject report or portion thereof," and, if so, the company must include "an explanation of the anticipated change, both narratively and quantitatively, and, if appropriate, state the reasons why a reasonable estimate of the results cannot be made."[120]

The NYSE can suspend trading in a company's shares and commence proceedings to delist a company that has not timely filed its periodic SEC filings.[121] A company then has a six month compliance period — which the NYSE can extend for a period up to another six months — to regain compliance with SEC filing requirements.[122]

Likewise, NASDAQ requires companies to timely file all required periodic reports with the SEC.[123] NASDAQ requires companies that fail to do so to submit a plan to regain compliance within 60 days. If NASDAQ accepts the company's plan, an additional cure period of up to 180 calendar days from the filing's due date can be provided to allow the company to regain compliance. In submitting such a plan, expect to provide a detailed summary of the investigation, a description of internal control and/or accounting weaknesses identified, and remedial measures.[124]

VIII. Paying For The Investigation

Internal investigations can cost millions of dollars. Not only does the company incur substantial legal fees, but it can also spend significant fees on e-discovery vendors, forensic accountants, and other specialists. In addition, individuals who are the target of the investigation or witnesses may incur their own legal fees, and the company may have an obligation to indemnify those individuals. Some of these fees and costs may be covered by a Directors and Officers Liability Policy ("D&O policy"). Rather than waiting until an investigation has been launched, counsel should review that policy now to understand the current coverage and options providing greater protection.

A. Indemnification And Fee Advancements

It is not uncommon for investigation witnesses to demand their own counsel. The question then arises whether or not the company has an obligation to reimburse the witness for her legal fees and costs. The answer typically is yes, as long as the company determines that the witness acted in "good faith" and in a manner that was in the best interest of the company."[125] Most company by-laws indemnify directors, officers, and employees for costs incurred in connection with an "action, suit, or proceeding." Delaware courts have held that internal investigations qualify as an "action, suit or proceeding" and are thus subject to indemnification.[126] And, even if the bylaws don't provide for indemnification, a company may decide to do so based on individual employment or indemnification agreements, the seniority of the employee, or past practices.

Because the determination of whether the witness acted in "good faith" and in a manner that is in the best interest of the company is not made until the investigation and any related litigation or proceedings are complete, companies often agree to advance fees as they are incurred. If a company agrees to advance fees, the witness must sign an "undertaking" to repay all advanced

fees and expenses if it is ultimately determined that she is not entitled to indemnification.[127] Once a company elects to advance expenses, it must do so until the exhaustion of all appeals.[128]

Until 2006, the Thompson Memorandum directed prosecutors to consider whether companies were advancing attorneys' fees to employees under investigation or indictment in determining whether those companies were cooperating. This provision of the Thompson Memorandum was harshly criticized as authorizing prosecutors to pressure companies to cut off legal fees for employees. After one federal court held that the Thompson Memorandum violated the Fifth Amendment Due Process Clause and placed an impermissible burden on employees' Sixth Amendment right to counsel, the DOJ modified its guidance to prosecutors.[129] The McNulty Memorandum, announced in December 2006, instructed prosecutors not to consider a company's advancement of fees when making a charging decision except in the extraordinary instances when the advancement, combined with other facts, constituted obstruction of justice.

B. Insurance

A D&O policy does not provide coverage unless a "Claim" has been made. "Claim" is a defined term under all D&O policies. Typically, it will include lawsuits, written demands for monetary relief, and administrative and regulatory proceedings. Because a pure internal investigation—one that does not involve a government investigation or shareholder demand—is none of these, legal expenses incurred in conducting the investigation are usually not covered.

But what if the internal investigation is triggered by a company receiving a subpoena from a regulatory agency? Or if, during the internal investigation, the company receives an informal request for information from the SEC? Or the company receives a demand from a shareholder to investigate alleged wrongdoing by some of its directors or officers? Whether or not these situations will be covered, and to what extent, will be determined by the D&O policy language.

1. Investigations Triggered By Government Investigations

Under standard D&O policies, costs incurred in responding to regulators' requests for information are often not covered. For example, in one recent, highly-publicized case, Office Depot conducted an investigation in response to an internal "whistleblower" letter and simultaneously complied with an informal SEC request for information. After the internal investigation was completed, the SEC issued a formal "order directing private investigation" and conducted a two-year investigation, which involved issuing subpoenas to eight former and current employees and officers and culminated in "Wells Notices" being issued to three officers. Office Depot then sought reimbursement of the $23 million it spent in legal fees and expenses in conducting the investigation and responding to the SEC's requests.

Reviewing the definition of "Claim" in the company's D&O policy, the court held there was no insurance coverage for costs incurred prior to the Wells Notice being issued. The policy's definition of "Securities Claim" specifically excluded "an administrative or regulatory proceeding against, or investigation of, an Organization." In addition, although the policy's definition of "Claim" included "a civil, criminal, administrative or regulatory investigation of an Insured Person," it only did so if the Insured Person was "identified in writing by" the SEC as a person against whom it might bring a civil proceeding. Because the SEC did not identify in writing the

specific individuals that it was considering charging until it issued the Wells Notices, any costs incurred by the Insured Person prior to the Wells Notice were not covered.[130]

Expanded claim language may, however, be available to cover all or some of these situations. Costs associated with a company's compliance with regulators' subpoena were covered, for example, where the company's D&O policy defined "Securities Claims" as including "a formal or informal administrative or regulatory proceeding or inquiry commenced by the filing of a notice of charges, formal or informal investigative order or similar document." In *MBIA, Inc. v. Federal Insurance Company*,[131] the Second Circuit held that a subpoena clearly qualifies as a "formal or informal investigative order," or at least as a "similar document," and thus triggered coverage.

In addition, insurers have recently begun offering coverage for investigation costs in their core policies or through endorsements. One carrier, for example, released a new D&O policy in 2010 that provides coverage incurred by individual insureds in responding to requests for interviews or documents from the SEC, DOJ, or similar authority. Other carriers have since followed suit by offering endorsements providing similar coverage. In addition, one carrier has also introduced a stand-alone policy designed to cover costs incurred by the company related to investigations by the SEC, DOJ, or similar authorities into securities violations (including investigations triggered by self-reporting). That carrier also offers an endorsement to provide a sublimit of coverage for investigations related to Foreign Corrupt Practices Act ("FCPA") violations.

2. Investigations Triggered By Shareholder Demands Or Derivative Lawsuits

As discussed earlier, investigations can be triggered by shareholder demands or lawsuits. In both of those situations, a board committee typically investigates whether claims should be brought against some of the company's directors or officers.

Standard D&O policies usually do not cover costs incurred in responding to a shareholder demand where a lawsuit has not yet been filed. A shareholder demand usually asks the board to investigate whether or not to bring a claim against a director or officer. Because no lawsuit has been filed and the demand is not asking for any relief, there has been no Claim made against any insured. If a derivative lawsuit has been filed, however, at least one court has held that costs incurred by a company's board in defending and investigating the derivative claims are covered.[132] At that point, claims have been made against insureds and the costs are related to defending against litigation.

Some D&O carriers offer additional insuring agreements providing for coverage for the company's investigation costs in responding to a shareholder demand or derivative lawsuit. That coverage is usually subject to a modest sublimit. In addition, some carriers have begun offering new policies and endorsements that provide coverage incurred by individual insureds in responding to requests for interviews or documents as a result of a derivative demand or lawsuit.

IX. Concluding The Investigation

When is an investigation substantially complete? When it meets these three requirements:

- The investigators are in a position to make findings, supported by the evidence, necessary to form the basis of the decision currently animating the investigation;
- The investigators can memorialize, transmit, and defend their conclusions to the internal and external constituencies who will use the findings; and
- The investigation provides a sufficient basis to remediate any weaknesses, deficiencies, or improper conduct identified during the investigation.

Each of these requirements is examined below.

A. Reaching Findings

Findings fall into one of three categories: process, substantive facts, and legal conclusions.

Process findings support the *adequacy* of the investigation. These consist of facts demonstrating that the investigation was properly authorized, scoped, and executed. The findings should include:

- The circumstances that triggered the investigation;
- The qualifications of the investigators;
- The interviews (the number of witnesses, their names, roles, and interview dates);
- The nature and scope of any expert work conducted (e.g., a description of the forensic accounting procedures applied);
- The quantity of documents and data collected, the names and roles of the custodians, and the review methodology; and
- The process by which those supervising the investigation kept apprised of developments, gave guidance to the investigators, and deliberated (e.g., the number and dates of audit committee meetings, supported by minutes).

Substantive factual findings describe what happened. What are the key transactions, events, or statements? Is there sufficient evidential support for the challenged disclosure, accounting treatment, or transfer? Did company personnel comply with internal standards and codes of conduct? Factual findings, and the documents and other evidence on which they are based, permit the organization to make the decision with which it is faced.

Finally, ***legal findings*** address whether the company, its directors, officers, employees, or contractors, violated federal, state, or foreign law. Investigators will usually *not* need to make such findings—and should think hard about doing so unless it's squarely required by the decision the organization faces. There is no requirement that a company, or its board, make legal conclusions or disclosures that are against its interests. To the contrary, Delaware (and other states) recognizes "the long-standing principle that to comport with its fiduciary duty to disclose all relevant material facts, a board is not required to engage in 'self-flagellation' and draw legal conclusions implicating itself . . . prior to a formal adjudication of the matter."[133]

A finding by the company that it violated the law, once disclosed, may be deemed an admission, with all the attendant negative consequences. Worse, the judicial system may ultimately disagree

with the legal findings regarding individuals or entities, exposing the company to further liability. Though the findings are no doubt made in good faith, new documents could emerge in civil discovery or a grand jury investigation, a judge could interpret the law differently, or the jury might end up believing that same witness the investigators found not credible.

There will of course be instances where an investigation must determine whether laws were broken; it will be the whole point of the effort. For example, a company may be investigating its involvement in a cartel for purposes of deciding whether to seek amnesty from the Antitrust Division. Or, the investigation may be conducted by a special litigation committee seeking to determine whether to prosecute claims on behalf of the corporation. But in most cases, the investigators will not have to formally conclude that the law was violated before the company can take action, whether a corrective disclosure, disciplinary action, a determination to restate, or even the decision to self-report an incident to law enforcement.

Remember, the tools available to the internal investigator are relatively humble. Internal investigators do not have subpoena authority over people or documents—they are powerless in the face of the recalcitrant employee who does not mind losing his job, the former officer who says she's too busy to appear for an interview, or the customer who declines to provide e-mails. The witnesses do not speak under oath and do not face the threat of perjury. True, investigators can draw inferences and must do their best with the available evidence. But it is usually prudent to leave the questions of legal liability to people whose ability to get the facts exceeds the internal investigation team: regulators, law enforcement, and juries.

B. Memorializing Conclusions

One way or another, the investigation's conclusions should be memorialized in writing so that there is a record of the investigation's diligence and so that the findings can be accurately communicated inside and outside the organization. This is often best done in the minutes of the meeting at which the investigation's conclusions are adopted. Here, a single document will capture the investigation's scope, procedures, any limitations on the investigation (such as unavailable witnesses, or the inability to rely on the authenticity of certain types of documents), factual findings, and recommended remedial measures (such as disciplinary action or corrective disclosures). It is usually wise to compile and have available at the meeting the key documents on which the findings are based.

Whether the detailed facts *underlying* the conclusions should be presented to the various constituencies in a written report, and who should receive it, present more difficult questions, discussed below.

1. Oral Versus Written Report

It is often presumed, incorrectly, that an internal investigation should conclude with a neatly typewritten and bound final report of the investigation, which includes all of the facts uncovered by the investigation. In reality, most of the time an oral report will not only suffice but will be preferable.

There are advantages and disadvantages to both. For example, a written report may be more easily understood and analyzed by its internal consumers, particularly in complex matters. But

that same written report can take on a life of its own. There is a greater risk it will, at some point, be transmitted outside of the organization involuntarily. Further, if the decision is made to self-report, regulators (and plaintiffs and auditors) will almost certainly request a written report and pressure the company to turn it over.

Here is a summary of some benefits and risks to consider before making a format decision:

Oral Reports

Pros	Cons
Usually less costly and completed quicker	Potentially viewed as less thorough
Less prone to hindsight criticism and second-guessing	Potential to be unclear and confusing, especially in complex cases
Will not find its way into wrong or unintended hands	Usually cannot be duplicated exactly for additional audiences
More easily protectable as privileged; lower risk of waiver	Not a roadmap for regulators; may be less helpful and lower cooperation credit
Nothing for regulators, auditors, and litigants to request	
Not a roadmap for third parties	

Written Reports

Pros	Cons

Generally viewed as more thorough and clear, especially in complex cases	Company "lives and dies" by the report—stuck with written word—more prone to hindsight criticism and second-guessing if not thorough enough or inaccurate
Seemingly more "professional"	Expensive and time-consuming
Can be easily provided to third parties (regulators)	Can be easily provided to third parties (plaintiffs)
Roadmap for regulators; may be viewed as more helpful and "cooperative"	Increased risk of privilege waiver if provided to third parties
	Will be requested by regulators, auditors and plaintiffs
	Roadmap for plaintiffs

2. Who Should Receive The Report?

a) The Board Of Directors

Depending on the nature of the investigation and the need for authority to implement the resulting recommendations, the investigative report may be presented to the Board. Typically, this is done through investigative counsel, with the assistance of any consultants. In some cases, management may receive a briefing about the findings before the Board meeting so that it will be prepared to address any accounting, disclosure, or operational consequences of the findings.

There are different ways to present the investigation report to the Board. Often, the investigators will give the directors a binder of key documents, the significance of which are explained as the investigative findings are described. Alternatively, a PowerPoint presentation with slides reflecting findings (and including images of key documents) may be projected but not distributed. If the Board receives written materials, the documents should be marked with control numbers, and a log kept of who received what information. Sometimes, given the risk of unintentional or unauthorized distribution, counsel will collect any written materials provided to the Board at the end of the meeting.

Because the discussion will be privileged, absent extraordinary circumstances, the directors should be instructed to clearly mark any notes they take as coming from a privileged communication involving counsel. Likewise, the appropriate section of the board minutes should be designated as a privileged attorney-client discussion, and reflect that the investigation report was delivered to and discussed by the directors. (The threats to privileged treatment of such presentations to the Board are discussed in Section X, *infra*.)

b) External Auditor

A company's auditors will have a keen interest in any internal investigation related to financial reporting or the integrity of officers and directors. And the auditor's views are important—if not satisfied, it can resign or it can withhold or delay its audit opinion or consent needed to keep SEC filings current. If any of these events happen, the company's private internal investigation will quickly become a public event. For those reasons, the external auditor is one of the most important audiences for internal investigation reports. At the same time, however, the company should try to satisfy the auditors without presenting analysis resulting in waiver of the carefully protected privilege. This can involve the careful delineation between non-privileged facts and work-product and legal analysis and advice.

c) Regulators And Law Enforcement

If the results of the investigation are reported to law enforcement or regulators, the form of that report will be an important decision. Again, the options are oral report, written report, or some combination of both.

The safest approach is to provide a purely oral presentation to the regulator (regardless of whether a privileged written report was made for the board of directors). In doing so, counsel can draw from their written report to ensure that all salient facts are covered in the discussion with the regulator. Actually turning over the work-product is rarely necessary. In most jurisdictions, turning over such work-product will result in a waiver as to both the regulator and third parties. Nevertheless, if government attorneys know there is a written report, they will likely want to see it. Although their value is highly questionable, confidentiality agreements with regulators, especially the SEC, are not uncommon.

In addition to the factual findings, the process and scope of the investigation must be explained, as well as the company's remedial steps. Along with the oral presentation, the company also may wish to produce non-privileged documents and interview list so the regulator can review the materials, speak with witnesses, and draw its own legal conclusion as to whether a violation has occurred. Make sure the regulator understands the scope of materials that are provided (and not provided) so there is no confusion down the road. If the company provides the appropriate facts, documents and access to witnesses, it should not be necessary for the company to turn over its privileged analysis to garner cooperation credit from regulators.

C. Remediation

If an investigation uncovers major problems, the directors and officers will be duty-bound to fix them by creating and implementing a robust remediation plan. That plan may mitigate corporate

penalties from regulators, be necessary to satisfy internal and external auditors, and help regain the trust of shareholders and other constituencies. Ideally a remediation framework will begin to develop as soon as a problem is detected so that, by the end of the investigation, all of the elements may be implemented promptly.

A remediation plan consists simply of the steps that should be taken to correct the problems (and in the cases of financial loss, to recover that loss). This may also involve steps to improve personnel, training, and internal controls to prevent similar future problems.

The development of these remedial measures will be ineffective unless their implementation is monitored and enforced. (Some settlements with the government require companies to appoint an independent monitor who reports to the agency, not management or the Board.) A clear post-incident process that breaks down all of the remediation steps should be prepared, with tasks and responsible persons assigned. Revisit the company's internal ethics and compliance program to determine whether they need revisions in light of the remediation plan. Regulators will pay close attention to whether the company actually implements the measures it has said it will take.

X. Protecting Privileged Communications And Work-Product

After taking careful steps to maintain the privileged nature of investigative communications and protect work-product, investigators may, for the organization's benefit, be required to share with third parties. The investigators should craft those third-party communications so as to avoid disclosing privileged or work-product materials and, when there is no choice but to disclose something privileged or protected, do it in a way that minimizes the waiver's scope.

A. Scope Of Protections And Waiver

It is helpful to have in mind the legal landscape of privilege against which disclosure decisions are made.

1. Attorney-Client Privilege

Investigators typically have many communications with directors, officers, and employees during the investigation that met the requirements of privilege as described in the Supreme Court's *Upjohn* decision.[134] Communications with forensic accountants and other experts who assisted during the investigation are likely also protected.[135] That's because "[a]ccounting concepts are a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases" and therefore "the presence of the accountant is necessary, or at least highly useful, for the effective consultation between the client and the lawyer which the privilege is designed to permit."[136] The privilege also may extend to public relations consultants.[137]

2. Attorney Work-Product

The investigation team likely created many materials during the investigation such as interview memoranda, notes, and spreadsheets. These materials are protected from the world by the work-product doctrine as long as they were prepared by (or at the direction of) attorneys in anticipation of litigation and for the purpose of analyzing the company's case.[138] The work-product doctrine should also protect intangible materials such as the attorney's or investigator's recollection of witness statements.[139] Information collected or communications made in the normal course of business, however, will not be protected.

Work-product protection is not absolute. But work-product reflecting an attorney's opinions, conclusions or mental impressions is discoverable only upon a showing of "extraordinary need or special circumstances."[140]

The company could be compelled to hand over ordinary work-product if the party seeking disclosure demonstrates "substantial need" for the materials and that it cannot obtain them by other means without "undue hardship." This is particularly true of work-product that is factual in nature, or prepared by non-attorneys. The party seeking disclosure can show "substantial need" if the facts in the attorney work-product are an essential element of its case and cannot be obtained elsewhere (*e.g.*, "contemporaneous statements taken from, or made by, parties or witnesses").[141] "Undue hardship" examines "the burden obtaining the information from an alternate source would impose on the party requesting discovery"—*e.g.*, "instances when witnesses cannot recall statements contained in interviews" or "[u]nusual expense involved in obtaining equivalent information."[142]

So while the work-product doctrine will not protect facts or the identity of witnesses from disclosure, it should protect whether an attorney or investigator has interviewed a particular person and the substance of the interview, precisely because that information would reveal the attorney's thoughts and strategy. This higher level of protection should also protect attorney notes and properly prepared interview memoranda in almost all circumstances.

3. Self-Critical Analysis

Most courts have rejected the privilege of self-critical analysis, or self-evaluation, for internal investigations. Those that have recognized it have applied it narrowly. Counsel should not rely on this privilege, but be aware of the arguments for it and keep tabs on changes in the law that may expand its availability and utility.

The self-critical analysis privilege is based on the public policy that it is beneficial for a company to be able to confidentially and candidly evaluate its compliance with laws. Information will not be protected under this privilege unless:

- It derives from a critical self-analysis;
- The public has a strong interest in preserving access to the type of information sought; and
- Access to that type of information would be curtailed if discovery were permitted.

The information also must have been prepared with the expectation that it would be kept confidential and has, in fact, been kept confidential.[143]

4. Waiver Doctrines

The attorney-client privilege and work-product protection can be waived through inadvertent or intentional disclosure of the protected materials. Work-product protection is "not automatically waived by any disclosure to third persons" but the question is whether the disclosure 'substantially increases the opportunity for potential adversaries to obtain the information. . . . Implicit in this analysis is the question of whether the third party itself can or should be considered an adversary."[144]

a) Disclosure: "Shield And Sword"

If the company puts a privileged communication from an investigation at issue in subsequent litigation, it will likely be required to disclose the substance of the communication in the litigation. This partial waiver stems from the idea repeated by many courts that the attorney-client privilege is a shield, not a sword.[145] It is thought that fairness requires the communication—and perhaps others related to it—be subject to examination.[146] Note that the waiver could be held to extend to related privileged communications, which means the company could be required to produce more materials concerning the subject matter, or be prevented from relying on the materials it failed to produce.

b) Subject Matter Waiver

This is the most important consequence of disclosure, and the one for which it is often difficult to predict its impact. If a company waives the privilege by disclosing a particular privileged document or communication, it could be compelled to waive the privilege over other related communications under the subject matter waiver doctrine.

The scope of the waiver should extend "only as to communications about the matter actually disclosed."[147] In *Chevron*, plaintiff argued that defendant waived privilege as to all documents relating to tax deferral question by disclosing two legal memoranda to the auditor involving subsidiary tax issues. The court found that the privilege was waived as to all communications concerning the subsidiary issues, but not to the more general tax deferral issue.

There are no precise rules governing how the scope of the subject matter waiver will be determined. As courts have noted, "subject matter can defined narrowly or broadly."[148] The analysis of the scope of the waiver typically requires a weighing of the circumstances of the disclosure, the nature of legal advice sought and the prejudice to the parties in permitting or preventing further disclosure.[149] Courts are "guided by the subject matter of the documents disclosed, balanced by the need to protect the frankness of the client disclosure, and to preclude unfair partial disclosures."[150]

B. Effect Of Disclosure To Third Parties

When companies disclose protected materials to a third party, they almost certainly waive the privilege as to the disclosed materials, and may also waive protection over other materials that cover the same subject matter covered by the disclosed materials.

1. Disclosure To Law Enforcement

Whatever privileged materials a company gives to law enforcement it should expect to have to provide to third parties in discovery in any subsequent litigation (as they will no longer be confidential). The more difficult question is whether the subject matter waiver effect of that disclosure can be blunted.

a) Selective Disclosure

In almost all circuits except one, companies cannot selectively disclose privileged documents to the government and expect to keep the privilege intact as to the disclosed materials. This is true even if the government provides a confidentiality agreement, at least for privilege if not for work-product. The Ninth Circuit is the most recent to reject the idea of selective waiver, holding that voluntary production of privileged information to the government waives the privilege, not just with respect to the government, but as to any other third party.[151]

The same rule—no selective waiver—holds in all the other circuits that have considered the issue: *United States v. Mass. Inst. Of Tech.,* 129 F.3d 681, 686 (1st Cir. 1997); *In re Steinhardt Partners, L.P.,* 9 F.3d 230, 236 (2nd Cir. 1993); *Westinghouse Electric Corp., v. Republic of Philippines,* 951 F.2d 1414, 1425 (3rd Cir. 1991); *In re Martin Marietta Corp.,* 856 F.2d 619, 623-24 (4th Cir. 1988); *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.,* 293 F.3d 289, 295 (6th Cir. 2002); *Burden-Meeks v. Welch,* 319 F.3d 897, 899 (7th Cir. 2003); *In re Qwest Commun. In'tl*, 450 F.3d 1179, 1197 (10th Cir. 2006); *Permian Corp. v. United States*, 665 F.2d 1213, 1221 (D.C. Cir. 1981); and *Genentech, Inc. v. United States Int'l Trade Comm'n*, 122 F.3d 1409, 1416-18 (Fed. Cir. 1997). In the Eighth Circuit, documents can be selectively disclosed to the government and the privilege can still be retained intact over them.[152]

b) Common Interest Doctrine

The so-called "common interest" doctrine creates an exception to the waiver rule under which disclosure of a communication to a third party will not waive privilege or work-product protection if it is in furtherance of a common legal strategy.[153] That is, "(1) made by separate parties in the course of a matter of common interest; and (2) designed to further that effort."[154]

This doctrine is unlikely to work with disclosures to law enforcement, however, since the private party cannot be said to be jointly strategizing with the government: he "has no more of a common interest with the government than does any individual who wishes to see the law upheld."[155]

c) Federal Rule of Evidence 502(A)

Relatively recent changes to the federal evidence rules may help minimize the impact of turning over protected materials. When privileged materials are intentionally disclosed to a federal office or agency so that any privilege or protection is waived, Rule 502(a) of the Federal Rules of Evidence extends that waiver "to an undisclosed communication or information in a federal or state proceeding only if . . . the disclosed and undisclosed communications or information concern the same subject matter . . . and . . . they ought in fairness to be considered together."

Under this Rule, a subject matter waiver is "reserved for those unusual situations" in which fairness requires a further disclosure of related, protected information, to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary."[156] In *United States v. Treacy*,[157] the court held that the law firm and its client did not waive work-product protection or attorney-client privilege over certain witness interview memoranda by disclosing others to the government. The court reasoned that the law firm "and its client, the Special Committee, have no adversary in this action, and there is no suggestion of 'selective' or 'misleading' conduct. To the contrary, all of the interview memoranda that were disclosed to the Government have now been provided to defendant. Accordingly, the instant case does not present any of the 'unusual circumstances' that otherwise would require a finding of waiver."

2. Disclosure To Auditors

The company's auditors may ask for protected materials in connection with doing its work on, and getting assurances as to, the company's financials. The disclosure of attorney-client privileged information to an outside auditor will likely be deemed a waiver of the privilege in most circumstances.[158]

Disclosure of work-product to an auditor, however, does not necessarily lead to a waiver. Work-product waiver is found where the disclosure is made in a manner that substantially increases the opportunity for potential adversaries to obtain the information. Some courts hold that work-product protection is waived by disclosure to outside auditors, because they perform an independent "public watchdog" function and thus their interests are not necessarily aligned with their client's.

But most courts take the view that disclosure does not substantially increase the likelihood for potential adversaries to obtain the information. Just because an auditor must be independent does not mean it is an adversary. These courts hold that disclosure of work-product to a company's outside auditor does not waive work-product protection because the auditor is not a litigation adversary and the interests of a business and its auditor are aligned in seeking to prevent, detect, and root out corporate fraud.[159]

C. Internal Company Communications

As discussed above, investigators often provide privileged materials to an organization's management team or board of directors at the conclusion of the work. Two Delaware Chancery decisions in a case called *Ryan v. Gifford* should be considered.[160] *Ryan* suggests that in certain circumstances—such as where the sitting directors of the board are defendants in a case involving

the matter under investigation—there may be risks of waiver in disclosing the results of an investigation internally.

In *Ryan*, a derivative plaintiff sued company directors, charging that the directors had breached their fiduciary duties by granting or accepting backdated stock options.[161] The company's board formed a special committee to investigate the allegations with outside counsel's assistance. At the conclusion of the investigation, the special committee presented a final report at a board meeting, attended by the directors' personal attorneys in the derivative case. Plaintiffs in the derivative case sought to compel production of the special committee's final report, as well as all communications relating to the investigation between the special committee and its counsel and between the special committee's counsel and the company.

The court ruled that the special committee had waived attorney-client privilege as to the report when it presented it at the board meeting attended by defendant directors and their personal attorneys. According to the court, the privilege was waived because the committee "disclosed its communications concerning the investigation and the final report to third parties – the individual director defendants and [their counsel] – whose interests are not in common with the client." The directors therefore were deemed to be third parties who fell outside the privilege.

Ryan may be criticized for its failure to take account of the full range of duties and obligations owed by a director to the corporation. For example, a director owes a duty to hold company information in confidence. The presence of a defendant director may argue for recusal, but it should not result in a waiver of the corporation's privileged communications. Indeed, at least one court flatly rejected the notion that a company's interested directors who receive the results of an investigation should be treated as "third parties" for purposes of a waiver analysis.[162] Moreover, a defendant director may be called upon to design, approve, or implement remedial measures. That is impossible to do in an informed, responsible manner if, to preserve privilege, the investigation's results must be kept secret from her.

XI. About the Authors

Morrison & Foerster's Securities Litigation, Enforcement & White-Collar Defense Practice Group is pleased to author this Internal Investigations InfoPAK in conjunction with the ACC. This InfoPAK reflects the contributions of lawyers across the firm, including Philip T. Besirof, Timothy W. Blakely, Jordan Eth, Dorothy L. Fernandez, Randall J. Fons, Mark R.S. Foster, Eugene Illovsky, Mark D. McPherson, Sean T. Prosser, D. Anthony Rodriguez, Robert A. Salerno, Daniel P. Westman, Anna Erickson White, and Miriam H. Wugmeister.

We have represented hundreds of companies and individuals in investigations involving alleged financial statement irregularities, disclosure issues, insider trading, the Foreign Corrupt Practices Act, and many other issues. Our practice group includes more than 125 attorneys, many of whom are former U.S. federal and state criminal prosecutors and SEC enforcement attorneys, working across 15 offices in the U.S., Europe, and Asia. Our team also includes an in-house Forensic Accounting Services Group.

We conduct cross-border investigations, perform reviews of prospective agents and joint venture partners, and represent companies and individuals in investigations by the U.S. Department of Justice, the SEC, and other enforcement agencies in the United States and elsewhere. While we handle focused, rapid investigations on a smaller scale, we also have the expertise, resources, and global reach necessary to perform large, complex investigations quickly and efficiently, anywhere in the world.

We also conduct compliance reviews and advise on policies and procedures, including real-time counseling to legal and compliance departments when problematic facts emerge. We design, review, and provide compliance training in local languages and, help companies develop remediation plans.

For more information, please visit **www.mofo.com** or contact the Co-Chairs of the Securities Litigation, Enforcement & White-Collar Defense Practice Group or the principal editor of this InfoPAK:

Jordan Eth
Co-Chair
San Francisco
(415) 268-7126
jeth@mofo.com

Randall J. Fons
Co-Chair
Denver
(303) 592-2257
rfons@mofo.com

Joel C. Haims
Co-Chair
New York
(212) 468-8238
jhaims@mofo.com

Carl H. Loewenson, Jr.
Co-Chair
New York
(212) 468-8128
cloewenson@mofo.com

Craig D. Martin
San Francisco
(415) 268-7681
cmartin@mofo.com

XII. Sample Forms & Policies

A. Sample Custodian Retention Notice

Case Name

CUSTODIAN INTERVIEW SHEET

PRIVILEGED & CONFIDENTIAL

A. GENERAL INTERVIEW INFORMATION

CUSTODIAN NAME: _____

1. Date of Interview:

2. Interviewer(s):

3. Location of Interview:

4. Introduce yourself and any other person with you.

5. Describe your role and explain privilege. For example: "I represent the Company. I do not represent you. I am conducting this interview to collect facts to provide legal advice to the Company. This interview is part of an investigation to determine the facts and circumstances surrounding [subject]. This conversation is protected by attorney-client privilege. But the privilege belongs to the Company, not you. Do not share the substance of this conversation with anyone, including other employees or third parties. The Company, and the Company alone, may decide to waive the privilege and share the substance of what we discuss here today with third parties, including the government. That decision is within the Company's sole discretion and will be made without notifying you." Afterwards, ask if the Custodian has any questions and is prepared to proceed.

6. Discuss with Custodian the *Document Collection Process Summary*.

7. Hand the Custodian a copy of the *Document Retention and Preservation Directive* and discuss scope and requirements. Obtain signed employee Acknowledgment.

B. CUSTODIAN INFORMATION

STAPLE

BUSINESS CARD

HERE

1. How long have you been at the Company?

2. What did you do before joining the Company?

3. Current responsibilities and title, including approximate start date of current position?

4. Do you have a current written job description? (Obtain a copy if possible.)

5. Prior position(s) within the Company and approximate time periods working in such position(s):

6. What regular meetings do you attend? How often do these meetings take place? Are you aware of any minutes, agendas, files or handwritten notes relating to these meetings? Where are these records kept or collected? Are the documents created put into project files on the server? (Get titles of project files on server)

7. What role, if any, in helping the company with this investigation have you had? Were you asked to pull together information, documents, etc.?

8. Who reports to you? Who do you report to? Has that changed since you have been in current position? (If so, ask for all names, departments or titles.)

9. Do you work with attorneys in-house or with any outside law firm?

10. Do you work with any state or Federal agencies (e.g. FDA, SEC, FTC, PTO, FCC, DOJ)?

11. Do you work with any subsidiaries of the Company?

C. LOCATION OF CUSTODIAN FILES AND/OR DOCUMENTS:

1. Do you have an assistant? Are they involved in your record keeping or sharing? (Get names and locations of all personnel and file locations).

2. What types of records or documents (letters, memoranda, notes, phone logs) do you typically generate?

   (a) Hard Copy:

   (b) Electronic:

3. Where do you typically store or backup your *non-e-mail* files?

   (a) Hard Copy:

   - Desk files?

- Central department file room?
- Off-site storage facility?
- Home (including your car or briefcase)?
- Other (supply rooms, cubicles, etc.)?

(b) Electronic:

- On your computer (e.g. folders under My Documents)? _____
- Network directory? _____
- In department folders? _____
- On share project folders on a server? _____
- Proprietary database? _____
- On CDs, DVDs, tapes, external drives? _____

4. Where do you typically store your current *e-mail* files?

- Network server?
- Personal workstation?

5. Where do you typically store, backup or "archive" *e-mail* or personal e-mail?

(a) On your computer? _____
(b) On your Home drive or personal network folder? _____
(c) On a departmental folders? _____
(d) On shared project folders on the Server? _____
(e) Proprietary databases? _____
(f) On CDs, DVDs, tapes, external drives? _____

6. Please identify other software you use and the file extensions that data generates.

7. Do you have any documents on-loan to any other employee?

8. Do you use a laptop and/or a computer at home?

9. Do you have or use any of the following?

Media	Yes	No	Location
External Hard Drives			
Zip/JAZ drive			
Laptop			
Floppy Diskettes			
CD-ROMS			
USB drives			
Tapes			
Flash Drive			
CD or DVD			
PDA (Personal Digital Assistants)			
I-Pod			
Home Computer			

Cell phone			
Blackberry			
Unapproved or unsupported software			

D. SPECIFIC DOCUMENTS REQUESTED:

1. Do you have any documents relating to [refer to specific areas of interest or topics]

2. Do you have any other documents that you think may be relevant to this investigation?

E. DOCUMENT RETENTION:

1. Approximately how long do you keep files?

   a. *Hard copy*:

   b. *Electronic*:

2. Has the Company's document retention policy been explained to you?

   a. *In writing*?

      (1) *Approximate date policy given*?

   b. *In person*?

      (1) *If yes, by whom?*

      (2) *If yes, approximate date explained?*

F. OTHERS THAT MAY HAVE ADDITIONAL DATA/FILES:

1. Predecessor (if more than one, write additional information on back):

   a. Name:

   b. Contact information:

      (1) Phone:

      (2) E-mail:

   c. Location of predecessor's files:

   d. Types of documents they may have/had:

2. What documents did you receive when you joined the Company?

3. Did anything you received from your predecessor go off to storage? Or, if the documents were retained, where are they located?

4. Have you been given anyone else's files? If so, where are those documents located? To whom did they belong?

5. Can you think of anyone else in the company who also may be in possession of documents or data that are relevant to the investigation? (Regardless of whether you think that we have already contacted him or her.)

6. Can you think of any former employees who may be in possession of documents or data that are relevant to the investigation? (Regardless of whether you think that we have already contacted him or her.)

7. Can you think of any third parties, other than former employees, who may be in possession of documents or data that are relevant to the invesitgation? (Regardless of whether you think that we have already contacted him or her.) Consider consultants, auditors, vendors, etc.

F. COLLECTION ACTIVITIES:

1. Hard copy document collection completed*?* YES NO NONE

   DATE: _____
   BY WHOM: _____

2. Electronically Stored Information collected?

   Workstation? YES NO NONE

   DATE: _____
   BY WHOM: _____

   Network Server? YES NO NONE

   DATE: _____
   BY WHOM: _____

   Other: _____ YES NO NONE

   DATE: _____
   BY WHOM: _____

B. Sample Document Collection Summary

TO: [Distribution List] (maintained by [Paralegal])
COPIES: [Relevant Legal Staff/ Senior Management]

FROM: [In-House Litigation or General Counsel]

DATE: [DATE]

RE: **DOCUMENT RETENTION AND PRESERVATION DIRECTIVE**
[Insert subject of internal investigation]

As you may know, the Company has commenced an internal investigation into [subject].

The Company takes this internal investigation very seriously and considers it a priority. [Law firm has been hired/Company counsel has been instructed] to assist and provide legal advice concerning this issue. If [law firm/Company counsel] is not provided with complete information, including documents, they will be unable to perform these services. **It is thus absolutely imperative** that we take immediate steps to preserve and retain, and to provide to [law firm/company counsel] as necessary, all records and documents that relate in any way to the subject matter of this investigation. Failure to preserve and provide potentially relevant documents could result in **extremely serious adverse legal, regulatory, and or financial consequences** for both the Company and responsible individuals.

Please be aware that it is the Company's responsibility to ensure that potentially relevant material is retained and that it is your responsibility as an employee of the Company to cooperate in every way with the retention process.

I. IDENTIFICATION OF DOCUMENTS

A. Subject Matter of the Investigation/Description of Relevant Categories of Documents

[*Insert a brief description of the scope of the investigation, including relevant date ranges and a broad listing of all categories of documents that could be relevant to the investigation.*]

B. "Documents" Defined

The term "Documents" includes, but is not limited to, agreements, correspondence, memoranda, notes (handwritten, typed, or otherwise), ledgers, work papers, informal files, desk files, handwritten notes, Post-its™, faxes, calendar entries (electronic or desk diary), address book entries (electronic or hard copy), and any copies, non-identical copies, drafts, alterations, modifications or changes to any of the foregoing.

"Documents" also encompass audio and video tapes; data stored on computer hard drives (including your office computer, personal home computer, or laptop), diskettes, CD-ROMs, DVDs, flash drives, as well as any and all other computer storage mechanisms; information in electronic format, including, but not limited to, voicemails, e-mails and any attachments to e-mails, instant messages ("IMs"), and other electronically stored materials. "Documents" also include files on cell phones, personal digital assistants ("PDAs"), and smartphones (such as, but not limited to, Blackberries® and iPhones).

If you are not sure whether a document is potentially relevant to the investigation and thus is subject to this preservation directive, err on the side of caution and preserve it. Also, if you are one of many recipients of an e-mail or other document that appears potentially relevant, please do not assume that one of the other recipients will preserve it – you should preserve it also. If you have any questions as to whether a category of documents is potentially relevant and should be preserved, please contact [Paralegal] at [contact info].

C. Locating Documents

Upon receipt of this Notice, you are required to locate and retain any and all hard copy and electronic documents and information in your possession, custody, and control that could be deemed relevant to this investigation (see Section I.A.). You should look for such documents in any location where you reasonably believe that they may be found (such as your office, your home computer(s), off-site archives, and any other location where you reasonably believe that such documents may be located.

If you are aware of other employees (including your secretary or assistant) who also may have documents relevant to this matter, please contact [Paralegal] immediately so that we may ensure that he or she receives a copy of this directive. In addition, if you are aware of the existence of relevant documents to which you do not have authorized access, please inform [Paralegal].

II. PRESERVATION OF DOCUMENTS

Once you have identified and/or located the relevant documents within your possession, custody, and control, it is your responsibility to secure them at once, i.e., do not destroy, discard, delete, modify, or remove any documents that are relevant to the subject matter of investigation, even if you would do so in the ordinary course of business.

It is not necessary that you physically segregate relevant files from your other working files, but you must clearly identify files that contain relevant documents and ensure that anyone other than yourself who works with those files also is aware that the files cannot be altered or destroyed in any way.

Upon receipt of this Notice, it is incumbent upon you to avoid destroying or deleting any electronic documents, voicemails, e-mails, or IMs. A technical team from our Information Technology Department will contact you in the very near future to explain how best to do this, but in the meantime, do not delete any emails stored in your Outlook mailbox or in a .pst folder, and please deactivate any inbox filters or rules that delete emails automatically. In the meantime, please contact [Paralegal] with any questions about the technical aspects of preserving potentially relevant electronic documents or preventing their destruction.

III. FUTURE OBLIGATIONS

The rules set forth in this Document Retention and Preservation Directive are effective unless and until you are informed otherwise in writing by [Author]. Until further notice, you should consider all document retention and/or destruction policies suspended with regards these documents.

Going forward, you must preserve all newly created hard copy or electronic documents that are relevant to the subject matter of the internal investigation and preserve them as described above. If you inherit documents from a departing Company employee, please review those documents for potential relevance and preserve them as instructed above.

V. CONFIDENTIALITY

All aspects of the Company's conduct of this internal investigation, including this directive and the identification and preservation of any relevant material related to the internal investigation pursuant to this directive, are communications and activities protected from disclosure by the attorney-client privilege and the work product doctrine. Please do not discuss any aspect of this internal investigation, including the documents and material that you locate and preserve, with anyone, **including others within the Company**, without having first spoken to [Author].

The Company greatly appreciates your assistance in this matter. If you have any questions concerning this request, please contact [Author] at [contact info] or [Paralegal] at [contact info].

C. Sample Document Collection & Process Summary

Thank the custodians for their time and cooperation in this process. Assure them that we will do everything in our power to make this process as painless and non-disruptive as possible. Also assure them that we are meeting with several people, i.e., they are not the only employee, and that our goal is to undertake a thorough one-time search for potentially relevant documents and electronic data. Let them know there is a chance we may need to talk to them again, but that this collection is an effort to obtain all relevant documents and data in one visit.

***DESCRIPTION OF MATTER*:** (TO BE DRAFTED BY INVESTIGATION TEAM)

***COLLECTION PROCESS DESCRIPTION*:**

A. Interviews are being done in person or by telephone by an attorney(s) and/or paralegal(s).

B. Potential document/file locations will be ascertained during interview.

C. A map of your office and file locations will be made by a member of the collection team.

D. Attorneys and/or Paralegals will look for documents in your office and all locations identified at time of interview (or at a scheduled agreed upon time).

E. When paper documents are removed from files, drawers, cabinets, etc., there will be a "dot" & "slip sheet" system used to identify you and location of each document removed. The paper documents are being electronically scanned by an outside vendor and may take a few days to return. When the paper documents are returned, they will be replaced in the same location from which they were removed. Colored dots and slip sheets will be removed by a member of the collection team. Please do not remove any of the dots or slip sheets until your files have been returned to their original locations.

F. A member of the Company's Legal Department and/or Internal IT Department will be calling you shortly to make arrangements for imaging data from your office computer, laptop, PDA, etc., and/or data from your home office, if applicable. It usually takes between one or two hours (sometimes less) to image one drive. We will make as many accommodations possible and try to limit the disruptions to you, your work flow and space.

OTHER POINTS TO CONFIRM:

 A. Do you understand that you should not withhold requested documents or data, even if you believe that the documents are privileged, duplicates, out of date, routine, drafts, or private?

 B. Do you understand the subject of the investigation and your obligation to preserve all documents and data that may be relevant? Do you agree not to destroy, delete or remove any potentially relevant documents and electronic data whether in paper format or electronic form?

☐ C. Do you understand that if you are uncertain whether a document or data is relevant to this investigation you should contact _____ of the Legal Department of the Company before destroying, removing, deleting, or altering anything?

☐ D. Do you understand that if you remember any additional information about relevant documents or data which may have been inadvertently deleted or destroyed, or that some relevant documents or data was not collected, you will inform an attorney member of the Company's Legal Department?

D. Sample Document Retention and Preservation Certification

DOCUMENT RETENTION AND PRESERVATION CERTIFICATION
[MATTER NAME]

EMPLOYEE COMPLIANCE STATEMENT

(This certification must be returned to [name and location] via email, even if you do not have any responsive material)

I read the above notice and conducted a reasonable search for any responsive documents. I certify that I am in compliance with the Document Retention and Preservation Directive, and I confirm that I understand I am to remain in compliance until I am specifically informed that the Directive is no longer in effect.

I further certify that I have searched the following locations for potentially relevant documents (Please check all boxes, as appropriate):

Search Completed	Location
	Laptop and/or office desktop
	Home computer
	Blackberry®, PDA, smartphone, and other similar handheld devices, including any of their saved folders
	Removable storage media, such as disks, CDs, DVDs, memory sticks, and thumb drives
	Personal hard copy files, including personal calendars, appointment books, and correspondence
	Electronic and hard copy files of any assistant or administrative personnel working for me
	Files located in my home
	Filing cabinets

Material Found:

_____	I have potentially relevant material and (mark all that are applicable):	
	_____	(a) stored my hard copy materials at **[location]**;

	_____	(b) stored my electronic materials at **[location]**.
_____	Based on a reasonable search, I have no potentially relevant material.	

_____ Name and I.D. Number	_____ Date
_____ Position	_____ Location

XIII. Additional Resources

A. ACC Docket Articles

"Risks and Rewards of Independent Internal Investigations," ACC Docket 29, no. 8 (Oct. 2010): 38, *available at* http://www.acc.com/legalresources/resource.cfm?show=1053036.

"Law School Didn't Prepare You for This Tips for the Internal Investigation," ACC Docket 28, no. 4 (May 2010): 58, *available at* http://www.acc.com/legalresources/resource.cfm?show=886141.

"Recent Trends in Internal Investigation," ACC Docket 25, no. 3 (April 2007): 24, *available at* http://www.acc.com/legalresources/resource.cfm?show=14544.

"HandsOn: Internal Investigations of Your Senior Executives," ACC Docket 24, no. 9 (Oct. 2006): 86, *available at* http://www.acc.com/legalresources/resource.cfm?show=14603.

"What to Do When the Whistle Blows: Do's and Don'ts of Internal Investigations," ACC Docket 22, no. 5 (June 2004): 40, *available at* http://www.acc.com/legalresources/resource.cfm?show=17030.

B. InfoPAKs

"Crisis Management in Litigation and Investigations: Parallel Proceedings, Competing Stakeholders, and Multiple Venues in a Global Environment," ACC InfoPAK (July 2011), *available at* http://www.acc.com/legalresources/resource.cfm?show=77428.

"Compliance Officer and General Counsel: Benefits and Pitfalls of Combining Roles," ACC InfoPAK (Sept. 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=995124.

"Implementing Legal Holds," ACC InfoPAK (Feb. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=19704.

C. Program Materials

"Ethics and Professionalism Issues Faced by Corporate Counsel When Dealing with Electronically Stored Information (ESI), Complex Discovery, Internal Investigations and Document Retention," ACC Presentation (Nov. 2011), *available at* http://www.acc.com/legalresources/resource.cfm?show=1299122.

"Corporate Internal Investigations: Key Legal and Practical Issues," ACC Presentation (Oct. 2011), *available at* http://www.acc.com/legalresources/resource.cfm?show=1296835.

"Conducting Corporate Investigations," ACC Presentation (June 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=966124.

"Role of in-house Counsel in an Internal Investigation," ACC Presentation (March

2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=19823.

"Internal Investigations, Practice Profile," ACC Presentation (Jan. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=19855.

D. Quick References

"Top Ten Tips for Conducting Effective Internal Investigations," ACC Top Ten (Nov. 2010), *available at* http://www.acc.com/legalresources/publications/topten/internalinvestigations.cfm.

"Internal Investigations Checklist," ACC List (Oct. 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=1213050.

"Top Ten Safeguards When Interviewing Employees During Internal Investigations," ACC Top Ten (Oct. 2010), *available at* http://www.acc.com/legalresources/publications/topten/internal-investigations.cfm.

"Recommended Practices for Companies and their Counsel in Conducting Internal Investigations," ACC Quick Reference (Feb. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=782287.

"Managing Internal and External Investigations," ACC Quick Reference (July 2007), *available at* http://www.acc.com/legalresources/resource.cfm?show=16527.

E. Other ACC Resources

"Internal Investigation Procedure and Guidelines," ACC Sample Form & Policy (May 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=930775.

"Internal Investigations Policy," ACC Sample Form & Policy (May 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=930832.

"Guidelines for Conducting Workplace Investigations," ACC Sample Form & Policy (May 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=931574

XIV. Endnotes

[1] Sarbanes-Oxley Act ("SOX"), Section 301(4), codified at 15 U.S.C. § 78j–1(m)(4).

[2] Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") Section 922, codified at 15 U.S.C. § 78u-6; Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, SEC Release No. 34-64545 (May 25, 2011) *available at:* http://sec.gov/rules/final/2011/34-64545.pdf. One recent whistleblower, for example, stands to receive nearly $20 million dollars for reporting a foreclosure fraud involving several major national banks. Jeff Feeley and David McLaughlin, *Bank Whistle-Blower Wins $18 Million Payday in Foreclosure Deal*, WASH. POST, March 16, 2012.

[3] SOX, Section 806, codified at 18 U.S.C. § 1514A.

[4] Dodd-Frank, Section 922, codified at 15 U.S.C.A. § 78u-6.

[5] SOX, Section 806, codified at 18 U.S.C. § 1514A; Dodd-Frank, Section 922, codified at 15 U.S.C. § 78u-6. The retaliation protections of Sarbanes-Oxley and Dodd-Frank are similar, but not identical. Under Sarbanes-Oxley, for example, an employee alleging retaliation must first file a complaint with the Secretary of Labor. If the Secretary of Labor has not issued a final decision on the complaint with 180 days, the employee may file suit in federal court. 18 U.S.C. § 1514A(b)(1). By contrast, the Dodd-Frank Act does not require employees to file a complaint with the Secretary of Labor before initiating suit in federal court. 15 U.S.C. § 78u-6(h)(B). The Dodd-Frank Act also provides that prevailing plaintiffs are entitled to double their back pay, whereas Sarbanes-Oxley provides only for actual back pay, without doubling. *Id.* § 78u-6(h)(C)(ii); 18 U.S.C. § 1514A(c)(2)(b).

[6] *See, e.g.*, N.Y. Lab. Law § 740(2)(a) (prohibiting retaliatory action against employee who "discloses, or threatens to disclose to a supervisor or to a public body an activity, policy or practice of the employer that is in violation of law, rule or regulation which violation creates and presents a substantial and specific danger to the public health or safety, or which constitutes health care fraud," among other protected activities); N.Y. Lab. Law § 215 (prohibiting retaliatory action against employee who makes a complaint concerning a potential Labor Law violation).

[7] 15 U.S.C. § 78j-1.

[8] *Id.* § 78j-1(b)(3).

[9] *In re Oracle Corp. Derivative Litig.,* 808 A.2d 1206, 1210 (Del. Ch. 2002) (citing *Zapata Corp. v. Maldonado*, 430 A.2d 779 (Del.1981)).

[10] Id.

[11] *London v. Tyrrell,* No. 3321-CC, 2010 WL 877528, at *12. (Del. Ch. Mar. 11, 2010).

[12] Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998); Faragher v. City of Boca Raton, 524 U.S. 775, 807 (1998).

[13] *Burlington Indus., Inc.*, 524 U.S. at 765 ("While proof that an employer had promulgated an anti-harassment policy with complaint procedure is not necessary in every instance as a matter of law, the need for a stated policy suitable to the employment circumstances may appropriately be addressed in any case when litigating the first element of the defense.").

[14] For instance, routine internal investigations may be authorized by any senior executive. Typically, these may relate to employment issues, commercial disputes, or violations of company policy. More serious issues—or issues relating to senior executives or directors—should be approved by the Board of Directors. A sample Board resolution authorizing an internal investigation is attached as _____.

[15] 17 C.F.R. § 205.3(b); *id.* at 205.2(i).

[16] *Id.* § 205.3(b)(3).

[17] *Id.* § 205.3(c).

[18] Id.

[19] *Id.* § 205.5.

[20] *Id.* § 205.5(d).

[21] The Seaboard Report, formally known as the "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions," was issued on October 23, 2001 as Release Nos. 44969 and 1470.

[22] *Id.* at ¶ 10.

[23] The Filip Memorandum is formally known as "Principles of Federal Prosecution of Business Organizations," (United States Attorneys Manual, Title 9, Chapter 9-28.00, effective August 28, 2008), *available at* http://www.justice.gov/dag/readingroom/dag-memo-08282008.pdf.

[24] *See* U.S. Department of Justice, Antitrust Division, Leniency Program, *available at* http://www.justice.gov/atr/public/criminal/leniency.html.

[25] U.S. Sentencing Guidelines Manual, Chapter 8, Introductory Commentary (2011).

[26] *See, e.g.*, *McCall v. Scott*, 250 F.3d 997, 1001 (6th Cir. 2001) (directors may be liable for "inattention" to and failure to investigate "red flags signaling fraudulent practices."); *Am. Int'l Grp Consol. Derivative Litig.*, 965 A.2d 763, 799 (Del. Ch. 2009) ("Our Supreme Court has recognized that directors can be liable where they consciously failed to monitor or oversee [the company's internal controls] thus disabling themselves from being informed of risks or problems requiring their attention.") (internal quotation marks omitted).

[27] 698 A.2d 959, 970 (Del. Ch. 1996).

[28] *Id*. at 969.

[29] *Id*. at 970.

[30] 15 U.S.C. § 7241; 17 C.F.R. § 240.13a-14; 17 C.F.R. § 240.15d-14.

[31] *See In re Guccione*, No. 3-11800, 2005 WL 146963 (SEC Admin. Proceeding Jan. 24, 2005) (instituting SEC cease-and-desist proceeding for filing a false certification); 18 U.S.C. § 1350 (imposing criminal penalties for the filing of a false certification); *see also* 18 U.S.C. § 1001 (imposing criminal penalties for making false statements to the federal government).

[32] 296. F.2d 918 (2d Cir. 1961).

[33] *See, e.g.*, ABA Model Rules of Prof'l Conduct R. 3.4 ("A lawyer shall not; (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act[.]")

[34] *See, e.g.*, *Hynix Semiconductor, Inc. v. Rambus, Inc.*, 645 F.3d 1336, 1347 (Fed. Cir. 2011); *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

[35] "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (internal quotation omitted) [*Zubulake IV*].

[36] *See, e.g.*, 18 U.S.C. §§ 1503, 1505.

[37] *Id*. at § 1519.

[38] *See, e.g.*, *United States v. Kernell*, 667 F.3d 746, 753-57 (6th Cir. 2012); *United States v. Yielding*, 657 F.3d 688, 711 (8th Cir. 2011).

[39] *See, e.g.*, U.S. Sentencing Guidelines §§ 3C1.1, 8C2.5(e); *see also id.* at § 8C2.5, Application Notes 9 ("Subsection (e) applies where the obstruction is committed on behalf of the organization; it does not apply where an individual or individuals have attempted to conceal their misconduct from the organization.").

[40] *Id*. at § 3C1.1, Application Notes 1; *see also* § 8C2.5, Application Notes 9 (referring back to Commentary to § 3C1.1 for guidance on conduct constituting obstruction).

[41] *See, e.g.*, *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622, 632 (D. Utah 1998) (fining defendant for failing to preserve e-mails of employees defendant had identified as possessing relevant information), *rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000); Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 Mich. Telecomm. Tech. L. Rev. 71, 77 (2004) (noting that monetary sanctions for spoliation, in the form of attorneys' fees and costs, were granted in 60% of cases surveyed).

[42] *See, e.g.*, *Bayoil, S.A. v. Polembros Shipping, Ltd.*, 196 F.R.D. 479, 482-83 (D. Tex. 2000) (striking defenses in light of "pattern of obfuscatory, misleading, and untruthful conduct," and finding that "whether or not there is a business justification for destroying documents, it is sanctionable to destroy documents when a party is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence") (internal quotation omitted).

[43] *See, e.g.*, *Blinzler v. Marriott Int'l Inc.*, 81 F.3d 1148, 1159 (1st Cir. 1996) (adverse inference appropriate where "a party is aware of circumstances that are likely to give rise to future litigation and yet destroys potentially relevant records without particularized inquiry").

[44] *See, e.g.*, *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 486 (S.D. Fla. 1984) ("Having determined that Piper intentionally destroyed documents to prevent their production, the entry of a default is the appropriate sanction."); *but see, e.g.*, Fed. R. Civ. P. 37(e) ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.").

[45] *See, e.g.*, *Zubulake IV*, 220 F.R.D. at 218; *Wm. T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984).

[46] *Vodusek v. Bayliner Marine Corp.*, 71 F.3d 148, 156 (4th Cir. 1995) (sanctions imposed).

[47] *See, e.g.*, *Danis v. USN Commcn'ns, Inc.*, No. 98 C 7482, 2000 U.S. Dist. LEXIS 16900, at *96–98 (N.D. Ill. Oct. 20, 2000).

[48] *Cf. Zubulake IV*, 220 F.R.D. at 218 ("[T]he duty to preserve extends to those employees likely to have relevant information -- the 'key players' in the case.").

[49] *Cf. In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) ("'[C]ontrol' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action.") (internal quotation omitted). For an in-depth discussion related to disclosing internal investigations to third parties, including potential issues related to the waiver of privilege or work-product protection, see Sections V.A.1.c, VII, and X.B.

[50] *See* The Applied Discovery Black Letter Book 3 (5th Ed. 2012).

[51] *Cf. Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) ("[I]t is necessary to thoroughly understand the responding party's computer system, both with respect to active and stored data.") [*Zubulake I*].

[52] *Cf. Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("[C]ounsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy.") [*Zubulake V*].

[53] *Cf. Zubulake IV*, 220 F.R.D. at 218 (noting that, as a general rule, the obligation to preserve does not apply to inaccessible backup tapes, but would apply to those actively used for information retrieval, and holding that "[i]f a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available").

[54] *See, e.g.*, Fed. R. Civ. P. 34(a)(1)(A) (allowing civil litigants to seek discovery of "any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form"); Fed. R. Evid. 101(b)(6) ("[A] reference to any kind of written material or any other medium includes electronically stored information.").

[55] See generally Zubulake V.

[56] *Cf., e.g.*, *Zubulake IV*, 220 F.R.D. at 218 ("[A] litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort), and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents.").

[57] The Applied Discovery Black Letter Book 3 (5th Ed. 2012) (citation omitted).

[58] Id.

[59] Id.

[60] *See Da Silva Moore v. Publicis Groupe & MSL Grp.*, No. 11 Civ. 1279 (ALC) (AJP), 2012 U.S. Dist. LEXIS 23350, at *6-7 (S.D.N.Y. Feb. 24, 2012) (citing Andrew Peck, *Search, Forward*, L. Tech. News, Oct. 2011, at 25, 29).

[61] *Id.* The order was subsequently affirmed by a United States District Court judge.

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

[63] The privilege analysis under state law may be different. *See*, *e.g.*, *D.I. Chadbourne v. Superior Court*, 60 Cal.2d 723 (1964) (applying 11-factor test).

[64] ABA Model Rule 4.3.

[65] ABA Model Rule 1.13(f); *cf.* Cal. Rule of Prof. Conduct 3-600(D).

[66] *See* ABA Model Rule 1.13; *cf. Responsible Citizens v. Superior Court*, 16 Cal. App. 4th 1717 (1993) (attorney-client relationship can be created by implied contract depending on circumstances including whether confidential information divulged and whether legal advice provided).

[67] *Upjohn*, 449 U.S. at 389.

[68] *See, e.g.*, *Three Rivers District Council and others v. Governor and Company of the Bank of England (No 6)* [2005] 1 AC 610 (H.L.) 642 ("Legal advice privilege covers communications between lawyers and their clients whereby legal advice is sought or given.") (U.K.); *R. v McClure*, [2001] 1 S.C.R. 445 (recognizing fundamental importance of solicitor-client privilege in Canada); *Waterford v The Commonwealth* [1987] HCA 25 (Austl.) (discussing legal professional privilege in Australia). In Hong Kong, the privilege even has a constitutional dimension: Article 35 of the Hong Kong Basic Law states that "Hong Kong residents shall have the right to confidential legal advice, access to the courts, choice of lawyers for timely protection of their lawful rights and

interests or for representation in the courts, and to judicial remedies."

[69] In civil law countries, the concept of "privilege" often comes from code-based professional confidentiality obligations imposed on attorneys.

[70] *See* Richard Bales, "Attorney-Client Privilege for Corporate Counsel Outside the U.S. and E.U.," presented at the May 8-12, 2011 Midyear Meeting of the American Bar Association's International Labor & Employment Law Committee (Berlin, Germany), *available at* http://www2.americanbar.org/calendar/ll0508-2011-midyear-meeting/Documents/bales.pdf.

[71] *See, e.g.*, *Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 64-66 (S.D.N.Y. 2010) (explaining analysis).

[72] *Id.* at 67 (citing *VLT Corp. v. Unitrode Corp.*, 194 F.R.D. 8, 16 (D. Mass. 2000)).

[73] *See generally Upjohn*, 449 U.S. at 389.

[74] *See, e.g.*, Richard Bales, "Attorney-Client Privilege for Corporate Counsel Outside the U.S. and E.U.," presented at the May 8-12, 2011 Midyear Meeting of the American Bar Association's International Labor & Employment Law Committee (Berlin, Germany), *available at* http://www2.americanbar.org/calendar/ll0508-2011-midyear-meeting/Documents/bales.pdf.

[75] *See Akzo Nobel Chemicals Ltd. v. Comm'n,* Case C-550/07 P [2010], *available at* http://www.acc.com/advocacy/upload/Akzo-decision-ECJ-14Sept2010.pdf.

[76] *Id.* ¶ 49. The court relied on the 1982 decision in *AM&SEurope Ltd. v. Comm'n of the European Communities*, Case 155/79, [1982] E.C.R. 1575, which recognized the privilege only between the company and "an *independent* lawyer entitled to practice his profession in a Member State" (emphasis added).

[77] LexMundi maintains a website that contains an analysis of whether communications with in-house counsel are protected by privilege under the law of various foreign (and U.S.) jurisdictions. *See* http://www.lexmundi.com/lexmundi/InHouseCounsel_AttorneyClientPrivilege_Guide.asp.

[78] Countries that have such comprehensive privacy statutes include: Australia, Hong Kong, Japan, New Zealand, South Korea, India, Singapore, and Taiwan in Asia; the European Union ("EU") Member States, Norway, Switzerland, Ukraine, Israel, Azerbaijan, Qatar, Angola, Senegal, Burkina Faso, Morocco, Albania, Croatia, Iceland, Liechtenstein, Macedonia, Moldova, Montenegro, and Morocco in Europe, the Middle East and Africa; and Argentina, Canada, Chile, Mexico, Paraguay, Peru, and Uruguay in North and South America. Many other countries are debating or considering such legislation, including Barbados, Bolivia, Brazil, China, Costa Rica, Ecuador, Jordan, Lebanon, Pakistan, Panama, South Africa, Sri Lanka, Tanzania, Thailand, Trinidad and Tobago, Turkey, and Venezuela.

[79] *E.g.,* Argentina, Denmark, Italy, Japan, and Spain.

[80] On January 25, 2012, Viviane Reding, Vice-President of the European Commission, unveiled a framework for a new EU data protection regime, which included a proposed Regulation which would apply directly to organizations and individuals and govern most data processing activities in the 27 EU Member States. *See* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[81] The EEA comprises the Member States of the European Union, plus Iceland, Liechtenstein and Norway.

[82] The 27 Member States of the EU are Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

[83] *See* Article 2(b).

[84] *See* Article 2(a).

[85] *See* Article 10.

[86] *See* Articles 7 and 8.

[87] There are other data protection principles and other obligations with which an organization must comply which are not relevant here.

[88] *See* Articles 25 and 26; also see further "3. Data Export Restrictions" below.

[89] It therefore applies to organizations in the following sectors: telecommunications, broadcasting, interprovincial or international trucking, shipping, railways, or other transportation, aviation, banking, nuclear energy, activities related to maritime navigation and shipping (including, for example, ports and longshoring), and local businesses in Yukon, Nunavut, and the Territories (where all private sector activity is in federal jurisdiction).

[90] Approval of the substantive provisions of the contract by most Member State DPAs is required if individually negotiated contacts (ad hoc contracts) are used. Contracts that incorporate certain standard contractual clauses approved by the European Commission ("Standard Clauses"), which cannot be modified by the parties, do not require DPA approval for the substantive provisions as they are deemed to be preapproved.

[91] See Article 1(2)(b) of the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related FAQs issued by the U.S. Department of Commerce.

[92] Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of October 24, 1995, adopted on November 25, 2005, page 15.

[93] For instance, not just those to which the data controller is a party (contrast the more restricted position under the legal basis of "necessary for compliance with a legal obligation to which the data controller is subject").

[94] The Eighth Data Protection Principle and international data transfers, version 2.0, page 25.

[95] Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of October 24, 1995, adopted on November 25, 2005, page 15.

[96] Hague Convention of 18 March 1970 on The Taking of Evidence Abroad in Civil and Commercial Matters, *available at* http://www.hcch.net/upload/appl-table20e.pdf.

[97] Hague Convention of 25 October 1980 on International Access to Justice *available at* http://www.hcch.net/upload/outline29e.pdf.

[98] Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal information to third countries, under Directive 95/46/EC, OJ (L181/19) of July 4, 2001, and Decision 2004/915/EC of December 27, 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal information to third countries, OJ 2004 (L385/74) of 2004.

[99] *See* Fed. R. Civ. P. 34 (permitting discovery requests for information "in the responding party's possession, custody, or control"); Fed. R. Civ. P. 45 (permitting subpoena to nonparty commanding production of information "in that person's possession, custody, or control").

[100] *See, e.g.*, *Cooper Indus. Inc. v. British Aerospace, Inc.*, 102 F.R.D. 918, 919 (S.D.N.Y. 1984) (ordering production from foreign affiliate, and imposing sanctions, because "[d]ocuments need not be in the possession of a party to be discoverable, they need only be in its custody or control").

[101] The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions became effective on February 15, 1999. *See* S. Treaty Doc. 105-43, 37 I.L.M. 1 (1999), *available at* http://www.oecd.org/dataoecd/4/18/38028044.pdf. As of May, 2012, 39 countries—including the United States—have ratified the OECD convention.

[102] For example, in 2002, the International Organization of Securities Commissions created a Multilateral Memorandum of Understanding, the first global multilateral information-sharing arrangement among securities regulators. Dozens of international securities regulators have signed the MOU, including the China Securities Regulatory Commission ("CSRC"), the United Kingdom's Financial Services Authority ("FSA"), the Hong Kong Securities and Futures Commission (SFC), the Monetary Authority of Singapore ("MAS"), Japan's Ministry of Economy, Trade and Industry, and the CFTC and the SEC in the United States. The International Organization of Securities Commissions reports that in 2010, the last year with reported data, more 1,600 requests for information were made pursuant to the MOU. *See* Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information, *available at* http://www.iosco.org/library/index.cfm?section=mou_main. The full text of the MOU is available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD126.pdf.

[103] *See* Section 21(a)(2) of the Securities Exchange Act of 1934, 15 U.S.C.§ 78u(a)(2).

[104] *See, e.g.*, Christine Caulfield, "DOJ Launches Antitrust Probe of Compressor Makers," Law 360 (February 19, 2009) (reporting European Commission dawn raids of several refrigerator and freezer compressor manufacturers in Europe, and concurrent dawn raids of facilities in the United States along with inquiries by competition authorities in Brazil and Italy).

[105] See U.S. Department of Justice Press Release, Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines: Coordinated Enforcement Actions by DOJ, SEC and German Authorities Result in Penalties of $1.6 Billion (Dec. 15, 2008), available at http://www.justice.gov/opa/pr/2008/December/08-crm-1105.html. The SEC's concurrent press release announcing the global settlement also emphasized the inter-regulator cooperation in the investigation of Siemens: it acknowledged contributions from the Office of the Prosecutor General in Munich, Germany, the UK Financial Services Authority, and the Hong Kong Securities and Futures Commission, as well as assistance from the DOJ, the FBI, the IRS. See SEC Press Release, SEC Charges Siemens AG for Engaging in Worldwide Bribery (Dec. 15, 2008), available at http://www.sec.gov/news/press/2008/2008-294.htm.

[106] *See* "The Serious Fraud Office's Approach to Dealing with Overseas Corruption," available at http://www.sfo.gov.uk/bribery--corruption/the-sfo's-response/self-reporting-corruption.aspx.

[107] *See, e.g.*, *CITIC Pac. Ltd. v. Sec'y for Justice* [2012] CACV 60/2011, at 38 ("Hong Kong law incorporates the concept of partial waiver of privilege."); *B and Others v. Auckland Dist. Law Society and Another* [2003] 2 AC 736 (P.C.) 761 ("It does not follow that privilege is waived generally because a privileged document has been disclosed for a limited purpose only." (UK law)).

[108] *See, e.g.*, *In re Paci. Pictures Corp.*, No. 11-71844, 2012 WL 1640627, at *3-4 (9th Cir. Apr. 17, 2012) (rejecting "selective waiver" theory adopted by the Eighth Circuit in *Diversified Indus., Inc. v. Meridith*, 572 F.2d 596 (8th Cir. 1978) (en banc) and noting that "every other circuit to consider the issue" has done the same).

[109] *See* Section 303 of the Sarbanes-Oxley Act (unlawful for personnel to "mislead any independent public or certified accountant engaged in the performance of an audit of the financial statements of that issuer for the purpose of rendering such financial statements materially misleading").

[110] In some cases, self-reporting of a potential violation is mandatory. *See* NYSE Rule 351 (requiring disclosure of, among other things, rule or law violations, and employee sanctions); 73 Fed. Reg. 67064, FAR Case 2007-006, Contractor Business Ethics Compliance Program and Disclosure Requirements (Nov. 12, 2008) (requiring government contractors to self-report credible evidence of violations of federal criminal laws involving fraud, bribery or gratuities and violations of the civil False Claims Act).

[111] *See* SEC Form 8-K, http://www.sec.gov/about/forms/form8-k.pdf, Item 4.02.

[112] *See* 17 C.F.R. § 229.103.

[113] *Id*.

[114] 17 C.F.R. § 229.401(f).

[115] *See* 17 C.F.R. § 240.10b-5 (implementing 15 U.S.C. 78j(b)).

[116] *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976) (setting the standard for determining whether an omitted fact is "material" and must be disclosed). Although *TSC Indus*. was decided under Section 14(a) of the Securities Exchange Act of 1934, 48 Stat. 895, 15 U.S.C. § 78n(a), the Supreme Court "specifically adopted, for the § 10(b) and Rule 10b-5 context, the standard of materiality" set forth in *TSC Indus*. *Basic Inc. v. Levinson*, 485 U.S. 224, 249 (1988).

[117] *See* NYSE Rule 202.05 (requiring a listed company "to release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities."); NASDAQ Rule 5250(b)(1) ("Except in unusual circumstances, a Nasdaq-listed Company shall make prompt disclosure to the public through any Regulation FD compliant method (or combination of methods) of disclosure of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions. The Company shall, prior to the release of the information, provide notice of such disclosure to Nasdaq's MarketWatch Department at least ten minutes prior to public announcement if the information involves any of the events set forth in IM-5250-1 and the public release of the material information is made during Nasdaq market hours. If the public release of the material information is made outside of Nasdaq market hours, Nasdaq Companies must notify MarketWatch of the material information prior to 6:50 a.m. ET. As described in IM-5250-1, prior notice to the MarketWatch Department must be made through the electronic disclosure submission system available at *www.nasdaq.net*, except in emergency situations.").

[118] 17 C.F.R. § 249.322.

[119] 17 C.F.R. § 240.12b-25.

[120] http://www.sec.gov/about/forms/form12b-25.pdf

[121] *See* NYSE Listed Company Manual, § 802.01E.

[122] *Id*.

[123] NASDAQ Rule 5250(c)(1).

[124] NASDAQ Frequently Asked Questions, Continued Listing the NASDAQ Market (November 19, 2008) (https://listingcenter.nasdaqomx.com/Show_Doc.aspx?File=FAQsContinued.html).

[125] See Del. Code Ann. Tit. 8 § 145(a) and (b).

[126] *See Hermelin v. K-V Pharm. Co.*, No. 6936-VCG, 2012 Del. Ch LEXIS 23 (Del. Feb. 7, 2012) (recognizing internal audit committee investigation qualifies for permissive indemnification upon showing of good faith); *Homestore, Inc. v. Tafeen*, 888 A.2d 204 (Del. 2005) (affirming indemnification of officer for internal audit); *Gentile v. Singlepoint Fin., Inc.*, 787 A.2d 102 (Del. 2001) ("no question" that internal investigations meet "the literal definition of a 'proceeding'").

[127] Del. Code Ann. tit. 8 § 145(e).

[128] *See Sun-Times Media Grp., Inc. v. Black*, 954 A.2d 380, 397 (Del. Ch. 2008) ("final disposition" means "final, non-appealable conclusion of a proceeding").

[129] *See United States v. Stein*, 435 F. Supp.2d 330, 364-65, 367 (S.D.N.Y. 2006).

[130] O*ffice Depot Inc. v. National Union Fire Insurance Company*, 2011 U.S. App. LEXIS 20759 (11th Cir. Oct. 13, 2011).

[131] MBIA, Inc. v. Federal Insurance Company, 652 F.3d 152 (2nd Cir. 2011).

[132] *Id.* at 162-166.

[133] *Stroud v. Grace*, 606 A.2d 75, 84 n.1 (Del. 1992) (citations omitted); *see also Loudon v. Archer-Daniels-Midland Co.*, 700 A.2d 135, 143 (Del. 1997) (directors' duty of disclosure "does not oblige them to characterize their conduct in such a way as to admit wrongdoing").

[134] *Upjohn Co. v. United States*, 449 U.S. 383, 396 (1981) (communications by Upjohn employees to counsel in internal investigation were covered by attorney-client

privilege). Federal courts now describe the privilege elements this way: "(1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection be waived." *United States v. Ruehle*, 583 F.3d 600, 607 (9th Cir. 2009) (citations omitted).

[135] *See, e.g.*, *United States v. Kovel,* 296 F.2d 918, 922 (2d Cir. 1961).

[136] *See also Gucci America, Inc. v. Guess? Inc.*, 2010 U.S. Dist. LEXIS 101219, at *34-35 (S.D.N.Y. Sept. 23, 2010) (*Kovel* "has been construed broadly to include individuals who assist attorneys in providing legal services, such as . . . technical experts, accountants, physicians, patent agents, and other specialists in a variety of social and physical sciences) (internal citations and quotations omitted). Note that some courts have held that the consultant must be acting as a translator or interpreter. *See, e.g., In re Refco Sec. Litig.*, 2011 U.S. Dist. LEXIS 113619 (S.D.N.Y. Sept. 30, 2011 (declining to extend privilege where there was no evidence the attorney could not understand information without the agent translating or interpreting raw data); *United States v. Ackert*, 169 F.3d 136, 140 (2d. Cir. 1999) (*Kovel* recognized that including a third party in attorney-client communications does not waive the privilege if the purpose of the third party is to "improve the comprehension of the communications between attorney and client," but declining to extend privilege where third party agent was not acting "as a translator or interpreter of client communications").

[137] *See In re Grand Jury Subpoenas Dated Mar. 24, 2003*, 265 F. Supp.2d 321, 331 (S.D.N.Y. 2003) (confidential communication with attorney-retained consultant for purposes of providing or receiving legal advice, not preserving a public image).

[138] *United States v. Noble*, 422 U.S. 225, 238-39 (1975); Fed. R. Civ. Proc. 26(b)(3).

[139] This may be true under state law as well. For example, in California, recorded witnesses statements are now, as a matter of law, entitled to at least qualified work-product privilege. *See Coito v. Superior Court*, 12 C.D.O.S. 7149 (2012).

[140] *Upjohn*, 449 U.S. at 401-02; *Garcia v. City of El Centro*, 214 F.R.D. 587, 591 (S.D. Cal. 2003) ("Opinion work-product, containing an attorney's mental impressions or legal strategies, enjoys nearly absolute immunity and can be discovered only in very rare circumstances.").

[141] *Fletcher v. Union Pac. R.R.*, 194 F.R.D. 666, 671 (S.D. Cal. 2000).

[142] Id.

[143] *See, e.g., Dowling v. American Haw. Cruises*, 971 F.2d 423, 426 (9th Cir. 1992) (declining to apply privilege to routine, voluntarily conducted safety reviews); *Slaughter v. AMTRAK*, No. 2011 U.S. Dist. LEXIS 10-4203, 2011 U.S. Dist. LEXIS 21838, *6 (March 4, 2011) (finding accident investigation report not protected; Third Circuit does not recognize the privilege).

[144] *Pulse Eng'g, Inc. v. Mascon, Inc.,* 2009 U.S. Dist. LEXIS 92971, at *10 (S.D. Cal. Oct. 1, 2009) (citations and internal quotation marks omitted).

[145] *Conkling v. Turner*, 883 F.2d 431, 434 (5th Cir. 1989) (citations omitted).

[146] *See, e.g.*, *United States v. Amlani*, 169 F.3d 1189, 1195 (9th Cir. 1999).

[147] *Chevron Corp. v. Pennzoil*, 974 F.2d 1156, 1162 (9th Cir.1992) (quotations omitted).

[148] See, e.g., In re Grand Jury Proceedings Oct. 12, 1995, 78 F.3d 251, 255 (6th Cir. 1996).

[149] S*ee, e.g.*, *Fort James Corp. v. Solo Cup Co.*, 412 F.3d 1340 (Fed. Cir. 2005) (there is "no bright line test" for determining subject matter of a waiver); *see also In re Grand Jury Proceedings,* 219 F.3d 175, 183 (2d Cir. 2000) (waiver of privilege is determined on a case-by-case basis); *United States v. Skeddle*, 989 F. Supp. 917, 919 (N. D. Ohio 1997) ("[d]espite the centrality of the term, 'same subject matter,' to this inquiry, courts have not defined its meaning and content precisely. Aside from a general instruction to construe 'same subject matter' narrowly, . . . no guidance has been given about how a trial court is to determine what is and what is not within the same subject matter when disclosure of some privileged communications has taken place.

[150] SNK Corp. of Am. V. Atlus Dream Entertainment Co., Ltd., 188 F.R.D. 566, 571 (N.D. Cal. 1999).

[151] *In re Pacific Pictures Corp.,* ___ F.3d ___, 2112 WL 1293534 (9th Cir. Apr. 17, 2012).

[152] Diversified Indus., Inc, v. Meredith, 572 F.2d 596 (8th Cir. 1977) (en banc).

[153] *Hunydee v. United States*, 355 F.2d 183, 185 (9th Cir. 1965).

[154] *United States v. Bergonzi*, 216 F.R.D. 487, 495 (N.D. Cal. 2003).

[155] In re Pacific Pictures Corp., 2112 WL 1293534.

[156] Fed. Rule Evid. 502 Advisory Committee Notes. *See*, *e.g.*, *In re United Mine Workers of America Employee Benefit Plans Litig.,* 159 F.R.D. 307, 312 (D.D.C. 1994) (waiver of work-product limited to materials actually disclosed, because the party did not deliberately disclose documents in an attempt to gain a tactical advantage).

[157] *United States v. Treacy*, 2009 U.S. Dist. LEXIS 66016 (S.D.N.Y. Mar. 24, 2009).

[158] *See, e.g., In re Pfizer Inc. Securities Litig.,* No. 90 Civ. 1260 (SS), 1993 U.S. Dist. LEXIS 18215, *22 (S.D.N.Y. Dec. 23, 1993) ("Disclosure of documents to an outside accountant destroys the confidentiality seal required of communications protected by the attorney-client privilege, notwithstanding that the federal securities laws require an independent audit.").

[159] See, e.g., *United States v. Deloitte*, 610 F.3d 129, 139 (D.C. Cir. 2010); *SEC v. Berry*, 2011 U.S. Dist. LEXIS 28301, at *24-25 (N.D. Cal. Mar. 7, 2011) (Lloyd, J.) (not for citation) (audit committee interview notes and memos); *SEC v. Schroeder*, 2009 WL 1125579, at *8-9 (N.D. Cal. Apr. 27, 2009) (Lloyd, J.) (not for citation) (PowerPoint and oral presentation); *In re JDS Uniphase Corp. Sec. Litig.*, 2006 WL 2850049, at *1 (N.D. Cal. Oct. 5, 2006) (unredacted board minutes).

[160] *Ryan v. Gifford*, No. 2213-cc, 2007 WL 4259557 (Del. Ch. Nov. 30, 2007) & 2008 WL 43699 (Del. Ch. Jan. 2, 2008)

[161] *Id*. (disclosure of special committee's investigation findings to board members being investigated and their personal attorneys waived privilege).

[162] *Picard Chemical Inc. Profit Sharing Plan v. Perrigo Co.*, 951 F. Supp. 679, 689-90 (W.D. Mich. 1996) (no waiver of attorney-client privilege or work-product by disclosing report to Board of Directors). *But see SEC v. Roberts*, 254 F.R.D. 371, 378 n.4 (N.D. Cal. 2008) (disclosure of a special committee's investigation findings constituted a waiver "since it was the Special Committee's mandate to ascertain whether members of the Board that may have engaged in wrongdoing").