O'Melveny | omm.com

IN-HOUSE COUNSEL'S GUIDE TO

Conducting Internal Investigations

What do you want to achieve?

It's more than what you do: it's how you do it.

Across sectors and borders, in board rooms and courtrooms, we measure our success by yours.

And in our interactions, we commit to making your O'Melveny experience as satisfying as the outcomes we help you achieve.

Our greatest accomplishment is ensuring that you never have to choose between premier lawyering and exceptional service.

So, tell us. What do you want to achieve?

TABLE OF CONTENTS

I. INTRODUCTION

In the wake of sustained government interest in corporate fraud and regulatory violations, expanding theories of corporate and individual liability, and the demands of auditors, internal investigations have become increasingly common. O'Melveny & Myers LLP has substantial expertise in handling such matters. O'Melveny's White Collar Defense and Corporate Investigations group also recognizes that the rise of the internal investigation is putting new pressures on in-house counsel—regardless of whether they decide to retain outside counsel to assist in a particular matter. In response to commonly asked questions from our clients, we have developed this guide to conducting internal investigations. It is not meant to be comprehensive; rather, it is a brief, practical guide meant to inform in-house counsel about key issues in a typical internal investigation.

This document does not constitute legal advice. It should be used as an aid in guiding internal investigations effectively and efficiently. You should consider the issues highlighted in this guide at the outset of an investigation as you (perhaps along with outside counsel) define the scope and goals of the investigation and create an investigation work plan and budget. As the investigation unfolds and facts are developed, you should continually reevaluate your investigation; it is often necessary to revisit and revise the work plan to ensure that it is meeting its goals.

This document outlines certain issues to consider, but does not purport to communicate bright line rules that must be followed in every instance. Each internal investigation must be tailored to its particular facts, circumstances, and issues. Few practices and protocols discussed in this guide are inflexible. When in doubt about what specific procedures to follow or actions to take, you should consult an experienced legal advisor.

II. OVERVIEW OF THE INTERNAL INVESTIGATION PROCESS

Most internal investigations progress through the following stages, each of which is discussed in this guide:

Opening the Investigation

- Triggering event(s)
- Deciding whether an investigation should be undertaken
- Deciding who should oversee and conduct the investigation
- Considering the need for outside counsel
- Considering the need for disclosure to and coordination with auditors, regulators, and others
- Designing the investigation with privilege protection in mind
- Considering immediate issues raised by the alleged misconduct and implicated by substantive law, geographic scope, and whistleblowers

Preserving Documents and Other Relevant Information

- Identifying custodians and corporate sources
- Preserving electronic data (including suspending automatic deletions)
- Distributing a document hold notice

Defining the Investigation's Scope and Procedures

- Developing a work plan and budget
- Establishing the division of labor among in-house counsel, outside counsel, and other parties
- Scheduling updates

Collecting and Reviewing Documents

- Collecting electronic data and hardcopy documents
- Conducting document collection interviews
- Deciding whether an electronic vendor or forensic expert is needed
- Processing and culling electronic data
- Setting up a review platform and choosing reviewers
- Developing a review protocol

Conducting Witness Interviews

- Scheduling and preparation
- Warnings for interviewees
- Counsel for interviewees
- Questioning techniques
- Interview notes and memoranda

Drawing Conclusions and Making Recommendations

- Evaluating the evidence (understand that facts evolve)
- Advising the person(s) overseeing the investigation
- Considering remediation
- Considering self-reporting

Closing the Investigation

- Presenting final report
- Implementing remediation plan

A. Triggering Events

The following events, among others, may trigger the need to investigate:

- Search warrants, receipt of subpoenas, or other requests for information
- Government interviews of current or former employees
- Media reports
- Whistleblower complaints or anonymous hotline or other internal reports
- Complaints from vendors, business partners, customers, or competitors
- Red flag in acquisition due diligence
- Shareholder demand or civil lawsuit (or threats thereof)
- Audit findings
- Board member request
- Industry-wide problems or government enforcement activity in industry
- Non-U.S. government investigations or enforcement activity, "dawn raid" of foreign subsidiary, affiliate, competitors, or business partners
- Widespread gossip or credible comments on social media or blogs

B. Should an Investigation Be Undertaken?

Some level of inquiry ordinarily is required in response to almost any allegation of misconduct. At a minimum, enough preliminary work should be done so that the company can make an informed decision about whether further investigation is necessary. There are situations in which an informal inquiry will suffice, but there are also situations in which good business judgment and common sense counsel in favor of a more extensive investigation.

A best practice is to thoroughly document the decision either way. If the decision is to stop after an informal inquiry, draft a privileged memorandum explaining the reasons why no further investigation is warranted. If the decision is to launch a more formal investigation, draft a work plan and budget document that defines the impetus for and scope of the investigation. To maximize the company's ability to claim attorney-client privilege over the investigation, this document should also state that the person(s) directing the internal investigation is in need of legal advice regarding the alleged wrongdoing and that counsel is being requested to conduct the investigation to develop factual information in order to provide this legal advice. To increase the likelihood of work product protection, the document should also state that the investigation is being done and advice is being sought in anticipation of litigation.

Below are a number of factors that should be considered before a final decision is reached:

- Source and credibility of information regarding alleged misconduct
- Nature of alleged misconduct, considering:
    - How severe is the alleged misconduct?
    - Is the alleged misconduct a one-time incident or a recurring issue?
    - Do the allegations involve potentially criminal conduct or wrongdoing or other violation of law, a routine compliance or employment issue, or a violation of employee code of conduct or other company policy?
    - Do the allegations implicate the integrity of management or involve possible financial reporting irregularities?
    - Is there potential for significant financial impact?
    - Do the allegations implicate the company's public image or contradict its public disclosures?
    - Is the company the victim?
- Type and history of company
    - Is it public?
    - Is the business closely regulated?
    - Is there a risk of debarment, suspension, or exclusion?
    - Have there been prior criminal or regulatory matters?
    - External pressures and critical audiences
    - Is this something that needs to be disclosed to the Board or Audit Committee?
    - Is there a pending government investigation? If not, would industry-specific government regulators, such as the FDA, Federal Reserve, or FAA, or more general government regulators, such as the U.S. Securities and Exchange Commission ("SEC"), the Department of Justice ("DOJ"), or state Attorney(s) General, be interested in the allegations?
    - Do the company's auditors need to know about a potential financial or disclosure issue? Could there be a management integrity issue?
    - Would a plaintiffs' law firm be interested in the allegations?
    - Will the results of the investigation impact time-sensitive disclosures or pending transactions?

- Do insurance carrier(s) need to be notified?
- Could the allegations have consequences with respect to lenders, bondholders, stockholders, business partners, or customers?
- Is there a whistleblower involved? Special considerations related to whistleblowers are addressed in Section VII, infra.
- What is the company's overall exposure or liability risk?

Some potential advantages of investigating:

- Allows management and Board to make informed decisions based on all of the relevant facts
- Promptly identifies the individuals responsible for the misconduct
- Provides mechanism to halt problematic conduct and prevent future violations
- Encourages improved compliance and culture
- May help company get out ahead of criminal or regulatory investigation or prosecution, preventing or significantly reducing potential consequences
- May enable company to avoid overly intrusive and lengthy government investigation
- May allow company to take advantage of potential benefits of cooperation
- May insulate company, Board, or management against allegations of complicity or of willful blindness to red flags
- May help in defense against shareholder claims

Some potential consequences of not investigating:

- Increased risk of criminal prosecution, regulatory enforcement action, or enhanced sanctions
- Increased risk of crisis or surprise when others uncover facts that an investigation could have revealed or remedied
- Increased risk of criticism and personal exposure for Board members and management
- Increased risk of a perception of a permissive corporate culture

Some potential downsides of investigating:

- Expense
- Disruption and distraction for business

- Discomfort for management or others who are the subject of or recused from investigation
- Risk that information uncovered will be discoverable in future litigation or will require government, regulatory, or public disclosure
- Public relations and market fallout from disclosure of investigation

C. Special Initial Considerations Based on Subject Matter and Other Special Circumstances

The nature of the allegations and the circumstances under which they arise may present additional considerations that should be analyzed at the outset.

- Do the allegations involve potential domestic or international antitrust violations? If so, the company's ability to qualify for corporate amnesty, whereby the company ordinarily escapes any fine, almost always turns on being the first company to disclose the violation to the appropriate enforcement agency. It is critical to conduct a highly expedited, yet thorough, investigation to determine whether the company may have criminal exposure for price-fixing, bid rigging, or other cartel violations. If the investigation reveals a potential violation, the company should strongly consider self-reporting and applying for corporate leniency.
- Do the allegations involve health care, life sciences, pharmaceuticals, or other areas that implicate patient or other third parties' safety? If so, consider whether there are practices that should be suspended pending the investigation.
    - Are patients' protected health information ("PHI") involved in the investigation? If so, PHI is subject to privacy and security laws and regulations that extend to lawyers and law firms representing healthcare entities. Data breaches of PHI can lead to separate government investigations, enforcement actions, and civil lawsuits.
- Do the allegations involve improper claims to federal healthcare programs? If so, the company may have a duty to identify certain overpayments and to make repayments. Carefully analyze repayment deadlines and triggering events to avoid further liability (e.g., 60 days after identification for Medicare and Medicaid overpayments).
- Do the allegations involve misuse of the company's or a competitor's trade secrets, or other data or confidentiality breach? Consider taking immediate steps to ensure that the company's and other confidential information is secure and to avoid potential exacerbation of initial misconduct (e.g., tainting of ongoing research or product development).
    - Nearly all states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring businesses to notify individuals when data security breaches compromise their personal information. Data breach notification laws are continually changing, with varying timelines for notification and differing disclosure requirements. The company should consider any applicable federal law and the statutes of all states in which they do business or of whose residents they have

personal information. Companies operating internationally should consider country-specific notification requirements.

- Do the allegations involve violations of U.S. export control laws? The investigation should include facts necessary to decide whether to voluntarily self-disclose to regulatory agencies, which may substantially mitigate penalties.
- Do the allegations involve possible payments (of any size or type) to foreign officials to influence official acts? The investigation should gather facts necessary to decide whether voluntary disclosure in an effort to mitigate penalties is warranted.
- Was the investigation triggered by a whistleblower? If so, it may be more likely that third parties will become aware of the allegations, and more likely that the disclosure occurs sooner rather than later. The more quickly the company investigates, the more prepared it can be to confront the issues in the resulting litigation or governmental inquiry.

  Other initial issues related to whistleblowers should also be considered:

  - Consider whether to inform the whistleblower that an investigation is being undertaken. If the whistleblower believes that the company is taking the allegations seriously, this could prevent or forestall disclosure to third parties.
  - Strict rules protect whistleblowers against retaliation. Make sure the identity of a whistleblower is not disclosed beyond those with a legitimate need to know, and remind all involved about prohibitions on retaliation.

  Special considerations will also arise when the time comes to consider interviewing the whistleblower and at the conclusion of the investigation. These issues are discussed further, in Section VII, *infra*.

IV. DECIDING WHO SHOULD OVERSEE AND CONDUCT THE INVESTIGATION

Once the decision to conduct an internal investigation has been made, the next step is deciding who should direct and conduct the investigation. This decision depends on who is being investigated, the type of wrongdoing at issue, and the resources needed to manage the investigation adequately. Many of the benefits of doing an internal investigation are contingent upon the real and perceived integrity of the investigation itself. Therefore, it is important to avoid any actual or apparent conflicts of interest. Process may be just as important as substance in internal investigations.

If the allegations implicate members of the Board of Directors, the Board should generally consider forming a committee of non-implicated directors (or, if necessary, new directors) to oversee the investigation. The directors' family, social, and business relationships with the subjects of the investigation should be carefully vetted. The committee ordinarily should retain an unaffiliated law firm of its choosing to assist it in conducting the investigation.

If the allegations implicate Section 16 or other high-level executive officers, a company should consider having the investigation overseen by the Audit Committee or other independent members of the Board of Directors. The directors on the committee ordinarily should choose an unaffiliated law firm to assist them in conducting the investigation.

If the allegations implicate non-executive managers or other employees, the General Counsel ordinarily may oversee the investigation. Whether outside counsel should be retained by the General Counsel depends on a number of factors, including the magnitude of the potential problem, the availability of in-house resources, and the need for subject matter expertise.

- The General Counsel ordinarily should not assume oversight responsibility if a legitimate argument could be made that the General Counsel has an incentive to inappropriately influence the investigation.
- Outside counsel should be considered if the allegations being investigated are potentially material to the company and might therefore trigger SEC reporting obligations.
- Consideration should be given to the likelihood that a court would conclude that the General Counsel was acting in a business, rather than legal, capacity, thereby threatening attorney-client privilege protection.
- If the General Counsel chooses to delegate the conduct of the investigation to another employee, such as the Chief Compliance Officer, it is important to document that the employee is acting at the direction of the General Counsel in order to assist the General Counsel in providing legal advice to the company.
- If possible, the company should ordinarily avoid placing responsibility for handling the investigation with the unit alleged to be involved in the conduct at issue.

Potential Investigators

If the Board or a Board committee is conducting the investigation, the Board or Board committee ordinarily should retain, as its independent counsel, a law firm that has not previously done work for the company. This may be required by the company's auditors and can serve to enhance the credibility of the investigation with government regulators.

If the General Counsel is directing the investigation, the decision whether to retain outside counsel is discretionary. The General Counsel may also choose to delegate the investigation to personnel in the company's compliance or internal audit department. When considering these alternatives, the General Counsel should consider, among other things, the potential impact on the attorney-client privilege and the credibility and quality of the investigation. Some factors to consider when selecting potential investigators are outlined below:

Investigation by Internal Audit

- May be experienced investigators
- Should be independent
- Report to management (concern about management inhibiting full disclosure)
- Communications may not be covered by attorney-client privilege[1]
- More appropriate in routine matters

Investigation by In-House Counsel

- Familiarity with the company's operations
- Less disruptive and less expensive to the company
- Experience with investigations varies
- May be seen as less independent by government regulators, shareholders, and other third parties
- Risk that some communications will be deemed business communications and not covered by attorney-client privilege
- More appropriate in routine matters, such as possible violations of employment laws and human resources issues

Investigation by Regular Outside Counsel

- Familiarity with the company's operations

[1] *See, e.g., United States v. ISS Marine Servs.*, 905 F. Supp. 2d 121, 129-39 (D.D.C. 2012) (rejecting privilege and work product claims over investigation conducted by internal auditor where outside counsel was minimally involved); *see also, e.g., Largan Precision Co v. Genius Elec. Optical Co.*, No. 13-cv-02502-JD, 2015 U.S. Dist. LEXIS 2072, at *15-17, *19-20 (N.D. Cal. Jan. 8, 2015).

- Attorney-client privilege will apply
- Lawyers' independence may be questioned given relationship with management
- Should not investigate matters in which firm was involved
- Should not investigate senior management or persons with whom the firm regularly works

Investigation by Independent Outside Counsel

- May be required in certain situations
- Attorney-client privilege will apply
- May have special expertise in internal investigations
- May have established credibility with government regulators or prosecutors
- May have less familiarity with business or operations than regular outside counsel

When outside counsel is retained, the engagement should be documented in writing. The engagement letter should clearly define the client, the allegations under investigation, and the scope of the investigation.

Relationship Between In-House Counsel and Outside Counsel

In most cases, it will make sense to designate an in-house attorney as a point person for the investigation, regardless of whether outside counsel is being retained by a Board committee or the General Counsel. Ordinarily, the designated in-house point of contact should be clearly outside the scope of the investigation and should not report directly or indirectly to anyone who might be within the scope of the investigation. If the entire legal department is conflicted, the point person should be outside the legal department. This person must have adequate experience and good organizational skills.

The in-house point person's duties will generally include assisting with the document retention and collection process, coordinating interviews, and monitoring the costs of the investigation, including the bills of outside counsel and any experts. Because serving as the point of contact for the various parties involved in an internal investigation can be time-consuming, overall workload should be considered in determining who will fill this role.

In situations where a Board committee with its own counsel is directing the investigation, in house counsel must be careful not to limit, or give the appearance of limiting, the scope of the investigation in any way, as this may jeopardize the investigation's credibility. At the same time, in-house counsel should be available to coordinate and assist with the committee's requests to the company. In-house counsel should also take steps to ensure that the committee's counsel is providing the committee with regular progress reports. It is important that the committee (not the committee's counsel) controls the investigation, makes key findings of fact, and draws conclusions.

In-house counsel may also be responsible for seeing that the company compensates directors for the time they spend on the investigation. Depending on the situation, committee members may be compensated per meeting, per hour, or with a flat fee. Per-meeting and flat fee compensation are the most common and least cumbersome methods.

Board Committees

If a Board committee is directing the investigation, the Board will need to pass a resolution authorizing the committee's work and nominating specific directors to the committee. The resolution should be passed as soon as practicable once the decision to conduct the investigation has been made. The Board resolution should include the reasons for the investigation, a finding that the directors named to the committee are sufficiently independent, and a clear description of the powers being delegated to the committee. In some situations, it may be necessary for the Board to delegate its full powers to the committee with respect to the matter being investigated, so as to buttress the committee's credibility and independence.

Separate Counsel for Employees or Officers

In some cases, it may be necessary or prudent to retain separate counsel for the individuals under investigation. This is particularly true in today's climate, in which DOJ has said that companies must report on "all individuals involved" in potential wrongdoing to obtain cooperation credit.[2] Counsel to the committee or person(s) directing the investigation should analyze the advantages and disadvantages of providing separate counsel based on the particular facts and circumstances. In-house or regular outside counsel should be asked to provide advice about the obligations of the company regarding indemnification and advancement of fees and costs to employees.

It is often advisable to obtain separate counsel for an individual when it appears that the individual is or may become a target of a criminal investigation. It also may be prudent to obtain separate counsel when some of the individuals involved in the underlying conduct will likely have an incentive to shift responsibility to a particular person or persons.

An advantage of retaining separate counsel for those under investigation is that witnesses will be better prepared and less likely to make inaccurate or untrue statements in their interviews. This is particularly significant where the company may be liable for the employee's conduct. Also, separate counsel can provide guidance to the individual about the advisability of submitting to an interview by government agents or asserting a privilege not to testify, which company personnel or counsel cannot do without triggering concerns of witness tampering or obstruction by the company or company counsel. Disadvantages of retaining separate counsel include the likelihood that the company may have less access to the employee and that doing so will likely materially increase the expense of the investigation.

---

[2] Sally Q. Yates, Remarks at New York University Law School Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (Sept. 10, 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

If separate counsel is obtained, consider the propriety of a joint defense agreement. Such agreements can help preserve confidential and privileged communications; however, be conscious of provisions that may restrict the company's ability to waive privilege in the context of cooperating with government agents or regulators.[3] A company or committee ordinarily will not want to compromise its ability to disclose to third parties information from an internal investigation as it sees fit. If the company seeks to preserve its ability to cooperate with the government, the company may consider a clause that allows it to make disclosures to the government, although doing so may limit the information it may obtain from the other parties to the joint defense agreement.

[3] *But see United States v. LeCroy,* 348 F. Supp. 2d 375, 387-88 (E.D. Pa. 2004) ("The facts of this case demonstrate that although entering into a JDA is often, indeed generally, beneficial to its participants, like skating on thin ice, dangers lurk below the surface.") (finding joint defense agreement between employee and company was modified by *Upjohn* warning, which included warning that company may disclose contents of interview to government, thus permitting company to disclose to government information uncovered during internal investigation interview of employee conducted by company's outside counsel).

V. PRESERVING THE ATTORNEY-CLIENT PRIVILEGE AND ATTORNEY WORK PRODUCT PROTECTION

The attorney-client privilege protects confidential communications between an attorney and client for purposes of giving or receiving legal advice. The attorney work product doctrine protects information, documents, and tangible things prepared in anticipation of litigation or for trial by or for one of the parties to the litigation or their respective counsel. One of the main reasons to have attorneys involved in an internal investigation is to preserve the confidentiality of the investigative record based on the attorney-client privilege or work product doctrine.

Key Steps to Preserving the Attorney-Client Privilege:

At the outset, properly document the purpose of the investigation. Include a statement that the individuals directing the internal investigation are in need of legal advice regarding the alleged wrongdoing and that counsel is being requested to conduct the investigation in order to provide this legal advice in anticipation of litigation.[4]

Attorneys should oversee the investigation. Where non-attorneys participate, they should make clear that they are acting under the direction of counsel for the purpose of providing legal advice to the company.

If a jurisdiction outside the United States is implicated, use outside counsel if the foreign jurisdiction's laws do not grant privilege protection to in-house counsel.

If the attorneys conducting the investigation retain an expert or consultant to assist them, the engagement letter should clearly document that the expert is working at the direction of attorneys in anticipation of litigation and in connection with their providing advice to the company.[5]

Refrain from mixing business and legal advice in the same communication.

Label documents (including emails) created during the course of the investigation with appropriate designations:

- Privileged & Confidential – Attorney-Client Communication
- Confidential – Attorney Work Product

Indicate the author and date of privileged or work-product protected documents.

Take reasonable steps to ensure that privileged and confidential documents created or discovered

[4] Internal investigations are sometimes undertaken for purposes of ensuring compliance with regulatory requirements and compliance programs, without necessarily the anticipation of litigation. At least one court has held that such investigations do not necessarily lose their attorney-client privilege protection: as long as obtaining legal advice is a primary purpose of the communications, the privilege applies even if there were also other important purposes (e.g., business or regulatory purposes). *In re Kellogg Brown & Root*, 756 F.3d 754, 759–60 (D.C. Cir. 2014). Although this opinion espouses a broad view of the attorney-client privilege, it is not binding outside the D.C. Circuit as of this writing. Thus, particularly because it is difficult to predict the forum in which a company might be sued, corporations establishing internal investigation protocols should not take for granted that other courts in other jurisdictions will hold a similarly broad view of the privilege. The steps outlined above, many of which were noted by the *Kellogg Brown & Root* court as significant indicia of a privileged investigation, should be followed. *See, e.g., In re Gen. Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 530 (S.D.N.Y. 2015).
[5] Attorneys who engage third-party consultants to assist them may share information without waiving privileges, so long as the consultants are assisting the attorney in providing legal advice. *United States v. Kovel*, 296 F.2d 918, 921-922 (2d Cir. 1961).

during the investigation receive confidential treatment:

- Limit distribution to those who need to know.
- Instruct recipients not to forward or disclose privileged or confidential communications.

During document review, segregate and tag documents that may be subject to a claim of attorney-client privilege or work product protection.

- Do not provide such documents to third parties.

At witness interviews, provide a clear *Upjohn* warning to employees and document in the interview memoranda that the warning was given. (*Upjohn* warnings are discussed in more detail in connection with witness interviews, in Section XIII, *infra*.) Make sure that witnesses understand that the investigation is confidential.

Do not use privileged or work product documents to refresh a witness's recollection.

Privilege may not attach to business advice provided in the course of conducting an internal investigation, such as advice on issues relating to termination of commercial relationships or employee discipline.[6]

As the investigation winds down, be wary of compromising the privilege. For example, some courts have found a waiver where privileged information about the investigation was shared with Board members who did not serve on the Board committee leading the investigation.[7]

Similarly, carefully consider the content disclosed to auditors, insurers, regulators, government agents, whistleblowers, and any other third party. Attorney-client privilege is unlikely to extend to these communications.

- Disclosure of investigative information to auditors may be required as part of the independent auditor's financial statement review and legal obligations. Auditors may not be able to sign off on a company's statements without knowing the results or findings of the investigation. Great care needs to be taken to accommodate the competing interests of attorney-client privilege and proper auditor disclosures. Consider providing auditors with oral factual summaries and information about investigative process, rather than privileged communications. Bear in mind that any information communicated to auditors will likely be memorialized in their work papers. Disclosures to auditors generally waive the attorney-client privilege, but not necessarily work product protection.

---

[6] *Koumoulis v. Indep. Fin. Mktg. Group*, 29 F. Supp. 3d 142 (E.D.N.Y. 2014) (communications between defendants and outside counsel regarding internal investigation of plaintiff's discrimination claims not privileged because predominant purpose was to provide human resources business advice).

[7] *See In re OM Group Sec. Litig.*, 226 F.R.D. 579, 590-94 (N.D. Ohio 2005) (PowerPoint presentation by audit counsel's outside counsel to entire board of directors regarding the findings of the ongoing investigation waived privilege); *SEC v. Roberts*, 254 F.R.D. 371, 383 (N.D. Cal. 2008) (communications between special committee's outside counsel and the board are not protected by the attorney-client privilege as the firm's client was the special committee, not the board itself).

- If disclosure to a government entity is contemplated, consider entering into a non-waiver or confidentiality agreement. Recognize that such agreements may not be enforceable against third parties, but they should be enforceable against the government entity that is a party and may afford some level of protection against third parties. It is likely that any information given to one regulator (e.g., SEC) will be shared with other regulators (e.g., U.S. Attorney's Office or DOJ) or even foreign governments (see Section VI, *infra*).[8] The sharing of "cyber threat indicators" with the federal government, however, will not result in a waiver of any privilege or protection provided by law.[9]

- Disclosure of privileged communications to third parties with a common interest with the client may be protected.[10] The common interest doctrine typically applies to co-parties in litigation, but some courts have also applied it to negotiating parties in corporate transactions (e.g., potentially permitting a seller who is conducting an internal investigation to disclose privileged information as part of due diligence to the buyer without waiving the privilege).[11] Whether the common interest privilege will apply depends on a number of factors, including the nature of the transaction, the timing of disclosure (e.g., disclosure to one suitor during diligence review versus multiple suitors during the initial stages of negotiations), the jurisdiction in which the waiver issue is litigated, and the steps taken to maintain the confidentiality of the information (e.g., whether a common interest agreement was executed, if access to privileged information was limited, if privileged information was transferred through counsel and not company executives, and if all privileged documents are clearly marked). Consider whether the information needed to advance the corporate transaction can be obtained from non-privileged sources such as presentations made to regulators.

Because there is no guarantee that the investigation will remain privileged, proceed with caution in all communications about the investigation. Assume that everything—emails, notes, invoices—could one day be subject to disclosure.

---

[8] Depending on the state of parallel government enforcement actions or civil litigation, consider seeking an order pursuant to Rule 502(d) of the Federal Rules of Evidence, which permits a federal court to order that the attorney-client privilege or attorney work product protection is not waived by disclosure connected with the litigation pending before the court, "in which event the disclosure is also not a waiver in any other federal or state proceeding." See, e.g., In re Gen. Motors LLC Ignition Switch Litig., 80 F. Supp. 3d 521, 526 (S.D.N.Y. 2015).

[9] 6 U.S.C. § 1504(d)(1) (Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act 2016, Division N), Pub. L. 114-113, codified at 6 U.S.C. §§ 1501-1510 (CISA)).

[10] The common interest doctrine, a limited exception to waiver, will apply where the parties undertake a joint effort with respect to a common legal interest, and the doctrine is limited to those communications made to further the common interest. See United States v. BDO Seidman, LLP, 492 F.3d 806, 815-816 (7th Cir. 2007).

[11] A New York appeals court recently confirmed that "[s]o long as the primary or predominant purpose for the communication with counsel is for the parties to obtain legal advice or to further a legal interest common to the parties, and not to obtain advice of a predominately business nature, the communication will remain privileged," even if the common interest does not stem from common litigation or the threat of litigation. Ambac Assurance Corp. v. Countrywide Home Loans, Inc., 124 A.D.3d 129, 135 (N.Y. App. Div. 2014) (overturning a lower court's order directing Bank of America to provide plaintiff with communications about the then-pending 2008 merger between the lender and Countrywide). See also Hewlett-Packard Co. v. Bausch & Lomb, Inc., 115 F.R.D. 308 (N.D. Cal. 1987) (holding that disclosure of attorney's opinion letter during negotiations for a substantial transaction did not constitute waiver); BDO Seidman, 492 F.3d at 816 n.6 (noting that six of the federal circuits recognize that the threat of litigation is not a prerequisite to the common interest doctrine). But compare Corning Inc. v. SRU Biosystems, LLC, 223 F.R.D. 189 (D. Del. 2004) (finding common interest doctrine not applicable where disclosures were made in effort to persuade third party to invest in defendant); Oak Indus. v. Zenith Indus., No. 86 C 4302, 1988 U.S. Dist. LEXIS 7985, at *11 (N.D. Ill. July 27, 1988) (declining to apply common interest doctrine to disclosures of confidential information during negotiations).

VI. SPECIAL CONSIDERATIONS FOR INTERNATIONAL INVESTIGATIONS

Where the investigation relates to events that occurred in whole or in part outside of the United States, additional issues are present. These issues include:

- Legal rules outside the U.S. that may impose different or additional substantive legal obligations on the company
    - The scope of the attorney-client privilege may differ by country. For example, the attorney-client privilege may not apply with respect to in-house counsel.[12] In some legal systems, attorneys who are not licensed in the jurisdiction may not enjoy the privilege with clients in that jurisdiction.[13] Careful consideration must be given to the privilege laws in the country in which the investigation is taking place.
    - At-will employment agreements may be supplanted by statute or contract.
    - Some countries require that appropriate individuals or entities, including a union or works council, be notified of an investigation, and potentially of the means that will be used to conduct the investigation.
    - Foreign labor and employment laws may provide employees with additional rights, including the right to insist on the presence at an investigative interview of a personal lawyer, a union or works council representative, and/or a company ombudsperson, colleague, or friend; the right to review a draft interview memorandum; or the right to challenge dismissal or adverse employment action. These rights may, in turn, impact the company's ability to preserve its attorney-client privilege.
    - Some countries prohibit anonymous tip lines. Additionally, anonymous evidence may be inadmissible as proof of violations.
    - Some countries require companies that discover wrongdoing to disclose it to the government.
- Privacy laws and regulations outside the U.S. that may impact the information gathering, interviewing, and document gathering related to overseas employees
    - Some countries restrict questioning about certain subjects (e.g., family or private relationships), and may prohibit interviews of employees altogether in certain circumstances.

[12] In *Akzo Nobel Chems. Ltd. v. European Comm'n*, Case C-550/07 P, Judgment of the Court at 9-11 (ECJ Sept. 14, 2010), the European Court of Justice found that, under European Union law, emails involving in-house counsel are not privileged, reasoning that in-house lawyers are not independent of the companies that employ them.

[13] The *Akzo Nobel* decision also confined privilege to attorneys who are licensed to practice law under the European Community regime. Communications between U.S. counsel and management in Europe are not privileged. When structuring an investigation that will involve Europe, U.S. outside counsel should consider involving counsel licensed to practice in the European Community in any witness interviews, correspondence, and other investigatory steps taken in Europe.

- In some countries, employees may not be required to cooperate with internal investigations, and cannot be disciplined for their failure to do so.
- Some data protection laws prohibit the collection and review of employees' "personal data," which may include company emails, without their consent. To secure the consent, the company may be required to provide the employee access to the information and give the employee the opportunity to correct any inaccuracies.
- Data identified for transfer to a third party for processing and analysis should be evaluated for personally identifiable information ("PII"). PII may need to be redacted or encrypted before transfer. The company may need to enter into data transfer agreements with third parties before sharing any PII.
- Some laws also prohibit or hinder the transfer of data outside the country of origin. Such "blocking" statutes may subject violators to civil fines and/or criminal penalties. Other countries require authorization from the local data protection agency prior to transferring data.
- Law in the foreign jurisdiction may differentiate between documents kept on servers in the United States and documents stored locally. Similarly, the company's obligations may be different with respect to email versus financial documents.
- Bringing documents and/or witnesses to the United States during the investigation may subject them to disclosure to private or government parties down the line, where they otherwise have been protected from such disclosure.
- China, in particular, has enacted a series of laws to safeguard information that may be deemed state secrets belonging to the state, provincial, or local government and state-owned enterprises. The export of data before it has been reviewed and cleared of state secrets can subject the company and its attorneys to severe administrative and/or criminal sanctions. To minimize the risk of violating the state secrets law, the company should consider conducting the entire document collection and review process in China, including a state secrets document review protocol.
- There are other Chinese laws that can hinder the collection and export of certain information—such as accounting archives, personal data, trade secrets, and bank secrets—for review outside of China. Also, certain due diligence and investigation practices to obtain information about Chinese individuals and companies may violate Chinese law.

- Potential enforcement actions by foreign governments, coordination or information sharing between U.S. and non-U.S. governments, and foreign execution of U.S. evidence requests under bilateral criminal judicial assistance agreements (and possible foreign investigation that may result from the execution of those requests)

- Foreign governments' amnesty or cooperation programs that have rules and applications different from that of the U.S.
- Need to employ translators during employee interviews

Due to these considerations, and the variation in the nature and effect of these types of laws in different jurisdictions, it is appropriate in most cases to seek the advice of outside local counsel in the countries at issue. If these international issues may be present, it may affect the choice of investigatory counsel at the outset. Engagement of an outside U.S. law firm with offices or expertise in implicated countries may reduce travel expenses and language or cultural barriers.

VII. SPECIAL CONSIDERATIONS RELATING TO WHISTLEBLOWERS

Various federal and state laws allow certain individuals to "blow the whistle" on company misconduct by reporting it to government agents, providing financial and other incentives to do so, and protecting whistleblowers from retaliation, including:

- Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), Sarbanes-Oxley Act ("SOX"), Foreign Corrupt Practices Act ("FCPA"), False Claims Act ("FCA")
- Provisions under consumer product safety, environmental, IRS, national security, occupational safety, workplace, or discrimination laws, transportation and infrastructure safety[14]
- State statutes; e.g., California Whistleblower Protection Act; New York False Claims Act

Some laws limit potential whistleblowers to particular categories of employees of certain types of employers, and protected activity includes limited types of misconduct; other laws are extremely broad. SOX whistleblower provisions cover a company's direct employees as well as private contractors and subcontractors.[15]

The culpability of a whistleblower does not prevent him or her from blowing the whistle.

Most laws provide remedies for retaliation against whistleblowers. These may include reinstatement, back pay, as well as interest and potential multipliers, litigation costs (including expert fees and attorneys' fees), and other damages.

Some laws provide for incentive payments, with whistleblowers potentially receiving a significant percentage of the sanctions that the agency is able to collect (fines, penalties, disgorgements, and interest). Under the Dodd-Frank Act, whistleblowers who voluntarily provide original information about a violation of federal securities laws that leads to an SEC enforcement action in which the sanctions recovered exceed $1 million are eligible for awards of between 10% to 30% of the money collected. FCA whistleblowers have also received sizable awards.

Some laws, such as the FCA, allow private persons ("*qui tam relators*") to file suit for violations on behalf of the government. Whistleblowers in other contexts also may bring direct civil actions against the company on their own behalf if they have been harmed.

Some laws do not require that the whistleblower report misconduct internally first; other provisions (e.g., SEC's Whistleblower Rules) incentivize internal reporting in some ways.

In light of whistleblower provisions in federal and state law, consider taking the following actions:

- Analyze the company's whistleblower policies and procedures, including anti-retaliation provisions, to ensure compliance with applicable laws.

[14] In April 2013, the Congressional Research Service reported that there were at least forty federal whistleblower and anti-retaliation laws. See Congressional Research Service, Survey of Federal Whistleblower and Anti-Retaliation Laws (Apr. 22, 2013), *available at* http://fas.org/sgp/crs/misc/R43045.pdf.

[15] *Lawson v. FMR LLC*, 134 S. Ct. 1158, 1176 (2014).

- Consider internal policies that encourage internal reporting, so that investigations can be undertaken before government involvement. This allows the company to "get ahead" of the problem, take corrective action if necessary, and be prepared with facts (which may be contrary to a later whistleblower report, or may be exculpatory in other ways) when the government comes knocking. Such policies may also allow for self-reporting before the whistleblower goes to the government, and/or the government may consider their existence and enforcement by the company as mitigating factors when evaluating any alleged wrongdoing. Examples of steps companies can take to encourage internal reporting include:
    - Instituting policies and training programs that can create a compliance culture, and highlight the value and importance of internal reporting.[16]
    - Making it easy for employees to report internally: for example, provide clear and simple instructions, repeated during trainings and other communications such as emails, handbooks, policy reminder memos, and postings; anonymous reporting provisions, hotlines, and clear lines of reporting, including a mechanism that allows employees to report to someone other than a direct supervisor.
    - Establishing anonymous hotlines for contractors, vendors, and clients.
    - Having employees periodically complete written certifications regarding their knowledge (or lack thereof) of unlawful or unethical conduct at the company.
    - Stressing the strength of the company's anti-retaliation policies during training sessions; make employees feel it is safe to report internally.
    - Ensuring that training, policies, employment and separation agreements, and employee confidentiality agreements do not discourage employees from reporting to the government.
- Have an action plan in place to respond quickly to whistleblower complaints. Whistleblowers who report a problem internally may have a condensed timeframe to also report to the government in order to qualify for a monetary award. If allegations are serious and have some indicia of credibility, the company may elect to self-report within that time period, even if the internal investigation is not complete.
- Where the identity of the whistleblower is not known, carefully consider non-discriminatory ways to quickly identify the source of the complaint. Consider involving the company's Human Resources department and qualified labor and employment counsel to ensure that the whistleblower is protected from retaliatory conduct.

[16] *See, e.g.*, Office of Inspector General, OIG Compliance Program Guidance for Pharmaceutical Manufacturers (68 Fed. Reg. 23,731) (May 5, 2003) (identifying seven essential elements for an effective compliance program).

- Carefully manage communications with the whistleblower during the investigation:
    - Consider informing the whistleblower that the investigation is being undertaken.
    - It may be appropriate to ask the whistleblower's view regarding the scope of the investigation.
    - Consider whether to interview the whistleblower, and, if so, when during the course of the investigation it makes sense to do so. In some instances, it may be appropriate to interview the whistleblower early in the investigation.
    - Use special care in a whistleblower interview and any other communications with a whistleblower.
    - In a whistleblower interview, in addition to an Upjohn warning, be sure to inform the whistleblower of the company's non-retaliation policy.
    - Depending on the circumstances, a whistleblower may not have a right to have an attorney present during the interview.
    - Consider how to proceed if the whistleblower refuses to be interviewed or otherwise cooperate with investigation. Under certain circumstances, hindering an investigation is not protected activity and can be met with discipline without triggering anti-retaliation laws. However, use extreme caution and consult with an employment lawyer before proceeding with any discipline against a whistleblower.
    - Be particularly thorough in a whistleblower interview: make sure the whistleblower is given the opportunity to voice all complaints, so the company is not surprised down the line with new or different reports to the government, and so the whistleblower's veracity can be tested and challenged as necessary.
    - Ask for or determine how to obtain all documents and evidence that support allegations from the whistleblower's point of view. All witnesses identified by the whistleblower should be considered for an interview.
    - Be conscious of the need to assess whistleblower credibility, but guard against immediate corporate or management reaction to mistrust the whistleblower.
    - Consider whether to keep the whistleblower updated on status during the investigation, especially if lengthy. Keeping the whistleblower informed may deter him or her from reporting the allegations outside the company or filing a lawsuit.
    - Consider informing the whistleblower that corrective action is being taken when wrongdoing is discovered. Even where the company concludes that there has been no material violation, consider informing the whistleblower of the outcome, without disclosing privileged information.

    - Be conscious of privilege issues in all communications with the whistleblower. Be aware that the whistleblower may be acting as a direct conduit of information to the government or plaintiffs' attorneys.

- Take special care to avoid retaliation or the perception of retaliation.

    - Retaliation can take many forms: termination, suspension, demotion, harassment, threats, discrimination of any form, denial of benefits or leave, fewer work hours or opportunities, subtle inequities, "anticipatory" retaliation, heightened level of scrutiny, or exclusion from meetings or projects.

    - Remind managers of anti-retaliation policy.

    - Do not disclose the whistleblower's identity or facts uncovered during investigations beyond those with a need to know.

    - Where adverse employment action is necessary due to unrelated conduct by a whistleblower, or where there is ongoing discipline that started before the whistleblower made his or her report, carefully balance the pros and cons of proceeding with such action or discipline. Terminating or disciplining an employee may affect continued cooperation. Consult with employment counsel and investigative counsel before proceeding.

VIII. DEFINING THE INVESTIGATION'S SCOPE AND PROCEDURES

At the outset, the person(s) in charge of the investigation should formulate a work plan and budget. If possible, the work plan and budget should be memorialized in a single, integrated document that can be referenced throughout the investigation. This document will help define the parameters of the investigation and clarify its goals. Details in the work plan and budget can, and should, be reevaluated during the course of the investigation as more information becomes known.

The investigation must be thorough enough to determine the scope of the improper conduct, identify the individuals involved, and determine whether management participated in, was aware of, or otherwise approved the conduct. The investigation must also withstand government scrutiny should the government learn of the conduct through self-reporting or some other mechanism. Although investigators ordinarily should not take a scorched-earth approach, they must follow the evidence. If, however, additional improper conduct is uncovered and not investigated, the investigation (and the company) may not be viewed credibly by the government.[17] And the company may need to conduct an even more expansive (and expensive) investigation under the government's direction.

A. Work Plan

The following topics should be outlined in the work plan portion of the document:

- Goal(s) of the investigation
- Scope
- General protocols
    - Preferred means and frequency of communication between outside counsel and committee or person(s) directing the investigation or outside counsel and in-house counsel. Those overseeing the investigation should consider methods of keeping investigation communications and documents confidential and secure.
    - Policy regarding communications between the person(s) conducting the investigation and persons within the scope of the investigation. Communications about the investigation should extend only to necessary individuals and counsel.
- Division of responsibilities
    - Types of tasks that will be performed by outside counsel. the committee, and in-house counsel.

[17] *See* Michael D. Goldhaber, *With Internal Investigations, Firms Walk a Tightrope*, THE AMERICAN LAWYER, May 26, 2016, *available at* http://www.americanlawyer.com/id=1202757857269/With-Internal-Investigations-Firms-Walk-a-Tightrope-?kw=With%20Internal%20Investigations%2C%20Firms%20Walk%20a%20Tightrope&cn=20160526&pt=Am%20Law%20Daily&src=EMC-Email&et=editorial&bu=The%20American%20Lawyer.

- Coordination with third parties
    - Auditors—discuss whether the company's auditors need to be kept in the loop about the investigation. Reasons for coordinating with auditors include a potential restatement or a potential management integrity issue. The fact that the auditors may need to be satisfied with the investigation is another important reason to include and consult with them regarding the investigation plan and initial scope at the outset. It is highly undesirable to get to the end of the investigation only to be told by the auditors that they disagree with how the investigation was conducted and that they want it to be redone. Transparency and regular communication as the investigation proceeds may help give the auditor confidence in the sufficiency of the investigation, the validity of the conclusions reached, and the appropriateness of any remedial actions. In some cases, the auditor may need to undertake additional audit procedures as a result of what is learned from the investigation. Carefully consider privilege issues in the context of auditor communications.
    - Regulators—discuss whether it may be necessary or desirable to self-report the investigation to the SEC, DOJ, or other authority. This is a complicated decision that should be thoroughly vetted with outside counsel. These issues are discussed further in Section XVII, *infra*.
    - Contractors or Vendors—discuss whether and to what extent third parties, such as contractors or vendors, who were involved in the underlying activity need to be involved in the investigation. For example, interviews of employees of third parties are ordinarily not protected by the attorney-client privilege absent a joint defense agreement.
- Major categories of tasks
    - Document preservation, collection, and review
    - Legal research
    - Factual development
    - Witness interviews
    - Expert evidence and opinions
    - Analysis and review
    - Consideration of remedial measures
- Desired deliverables or range of outcomes—report, disclosure, mediation, settlement, etc.

B. Budget

The budget should generally track the steps outlined in the work plan and include the following:

- Coordination of investigation
- Preservation and collection of documents
    - Suspending normal document destruction practices
    - Implementing automatic archiving, if necessary
    - Imaging hard drives and servers
    - Copying hardcopy files
    - Converting collected files into usable format
    - Retaining a forensic expert, if necessary
- Document review
    - Attorney time
    - Costs of the review tool (software)
    - Possible retention of a service provider with automated review capabilities
- Witness interviews
    - Attorney time
    - Travel and other associated expenses
- Experts or consultants
    - Forensic accountants
    - Subject matter experts
    - Computer forensic experts
    - Consulting attorneys
- Separate counsel for individuals within the scope of the investigation
- Preparation of reports and recommendations
- Interaction with government entities or other authorities
    - Attorney time
    - Document production, including privilege review

- Remediation
    - Corporate governance changes
    - Personnel changes
    - Compliance program or training

Make sure that the person(s) in charge of the investigation understand and approve staffing, billing rates, and retention of experts.

C. Initial Legal Analysis

Some investigations may require initial, limited legal research and analysis to help define the scope of the investigation and identify potential risks presented by the allegations of wrongdoing. In such instances, it may be advisable for counsel to draft a memorandum outlining the legal landscape and providing initial analysis based on preliminary facts. As the investigation progresses and additional facts are developed, counsel may update the memorandum to the extent newly uncovered facts change the legal analysis or require additional research to frame the legal issues and assess potential risks.

To ensure that any such memorandum remains protected as attorney work product, it should typically be maintained by outside counsel. The analysis recorded in the memorandum may be shared verbally with select individuals within the company, but broad dissemination of the memorandum should be avoided to preserve the protections of the attorney work product.

D. Use of Experts

In some cases, it is helpful to retain experts to assist in the conduct of the internal investigation. If a significant amount of electronic data needs to be collected, for example, counsel should strongly consider retaining a computer forensic expert. The expert will be able to forensically image hard drives, so that deleted files and metadata are preserved. The expert will also be able to testify about the methods of collection if there is ever a dispute about chain of custody or data authenticity.

Depending on the factual allegations at issue, it may also be prudent to retain subject matter experts. In an internal investigation involving accounting fraud, for instance, forensic accountants are likely to be helpful. Similarly, executive compensation consultants, ethics experts, safety experts, economists, or damages experts may be an asset in particular investigations. Other individuals with specialized knowledge, such as industry or regulatory experts, can also be useful during an internal investigation.

Agents working under the direct supervision and control of the lawyer may be included in the scope of the attorney-client privilege, if their services are a necessary aid to the rendering of effective legal services to the client. As a general rule, to preserve attorney-client privilege and work product protection for the investigation, experts should always be retained by counsel

conducting the investigation, regardless of whether the company is directly billed for their services. The engagement should be documented in writing. It is also critical that due diligence is performed on any expert before he or she is retained. Counsel should inquire about the expert's experience in similar matters and consider any factors that may undermine the expert's credibility. If the expert will be doing a significant amount of work, counsel may wish to ask for and speak with professional references. Once an expert is retained, counsel should closely oversee and direct the expert's work. Communications between experts and company employees should be made at the direction of counsel to gather information to aid counsel in providing legal services.

Issues may arise if the expert in question has preexisting ties to the company or individuals investigated. Such ties can present conflicts of interest or the appearance thereof. For example, in an internal investigation involving accounting fraud, the company's regular outside accounting firm has an obvious conflict of interest in the results of the investigation.

Finally, experts who are employees of the company present special complexities relating to privilege. Because a non-legal employee's day-to-day communications and work are not privileged, it can be difficult to show which aspects of the employee's work were performed in the employee's capacity as an employee (and thus are not privileged), and which were performed in the employee's capacity as an expert assistant to counsel (and thus are privileged). However, in some cases, particularly investigations involving trade secrets or highly technical business information, internal experts may be the only practical sources of expert knowledge. If such experts are ultimately utilized, counsel should take basic precautions to protect the privilege. These precautions include ensuring that all work the employees do in their capacity as experts is clearly marked as privileged, and that the employee keeps separate files for privileged and non privileged materials.

E. Methods of Investigation

Document review and witness interviews are the most common ways of gathering information during an internal investigation. It is the rare case where surveillance or monitoring is warranted. Because activities such as video surveillance, phone taps, and monitoring of computer use may run afoul of privacy laws in many jurisdictions, they should be undertaken with extreme caution and only after consultation with outside counsel. By the same token, attorneys conducting an investigation should be wary of using deceptive tactics to elicit information or incriminating statements from those being investigated. If a matter seems to call for such extreme measures—e.g., suspected insider trading—the company should consider contacting the appropriate enforcement authorities.

IX. DOCUMENT PRESERVATION

Although we have identified discrete steps below, they should be executed in parallel to the extent possible.

Step One: *Identify Custodians and Sources.* In-house counsel, and, if applicable, the company's regular outside counsel, and independent counsel to the person(s) overseeing the investigation, should work together to develop a list of persons who may have relevant documents. In creating this list, refer to the following tips:

- Use organizational charts.
- Use scoping interviews to determine additional custodians who may have relevant documents.
- Consider including former employees, Board members, administrative staff, outside consultants, outside counsel, accountants, team members, vendors, suppliers, etc.
- Consider non-custodial sources of documents, such as corporate records, accounting systems, HR records, etc.
- Revisit the appropriate custodians and sources as the investigation continues to determine if others should be added; consider reviewing a sample of documents from potential additional custodians to estimate the cost of collecting additional custodians.

Step Two: *Contact the IT Department*. In-house counsel should contact the department in charge of the company's technology to inform them that an internal investigation is beginning. Given the various formats, platforms, and dispersed locations in which electronic records are stored, it can be a challenge to locate potentially relevant material. In-house counsel and IT personnel or outside consultants should take the following steps:

After identifying an initial set of custodians, collect the electronic data sources from those custodians, including taking images or extracts of user hard drives, mailboxes, My Documents folders, and other personal drives located on the company computer network. To help facilitate collection, the IT Department should also compile a list of physical inventory and removable media—laptops, tablets, smartphones, telephones, etc.—in the possession of identified custodians.

- Remember that relevant documents may also be preserved on a custodian's personal device, home computers, or portable media, such as USB drives.[18]
- System shared drives also may need to be preserved.
- Active data includes email, standard business documents such as word processing files and spreadsheets, text messages, instant messages, chats, phone records, and voice mail.
- In many cases, it is desirable to preserve metadata and deleted documents, not merely active files on the custodian's hard drive.

[18] While gathering information about employee devices, consider the terms of the company's computer usage and "bring your own device" policies, including whether consent is required to collect data from personal devices.

Suspend regularly scheduled purges of deleted data on servers that may contain relevant documents, including the message management auto-delete configuration on individual custodians' email accounts. Consider whether automatic archiving needs to be activated to preserve newly generated data.

Work with IT personnel to develop an appropriate preservation plan for inactive, archived, residual, and legacy data. Otherwise, it is common for backup media to be rotated and overwritten, and archived data to be automatically deleted after a specified time period. It can be costly and burdensome to identify archived data, to pinpoint where and how data is stored, and to restore the data into usable formats. The obligation to preserve documents and electronically stored information requires reasonableness and good-faith efforts, but companies may not need to preserve data that is only remotely relevant or extremely difficult to access. Carefully consider whether there is relevant archived data that warrants the expense and effort of collection and processing. Counsel can help set reasonable and defensible limits in preserving and collecting documents.

The hold and suspensions should generally remain in effect until at least the conclusion of the investigation. If litigation is reasonably foreseeable, holds and suspensions should remain in effect after the close of the investigation. Counsel and the IT Department should routinely revisit and monitor the hold process.

Step Three: *Distribute Litigation Hold Notice.* The General Counsel should distribute a comprehensive, comprehensible litigation hold notice to the identified custodians, instructing recipients to preserve all potentially relevant documents. Factors to keep in mind in drafting and updating the hold notice include the following:

- The hold notice should typically provide high-level background explaining the reason document preservation is necessary. For example, if the company is being investigated by the government, the hold notice should ordinarily include that information.
- Use plain language and give practical instructions. Consider sending notice in the body of an email (rather than an attachment) so that employees are more likely to read it.
- The categories of documents preserved should be broad enough to cover all potentially relevant information without being vague. Give concrete examples of the types of information that must be preserved. Attempt to consolidate or summarize various categories of documents to make the instructions easier to follow. Where a subpoena or government request is the reason for the hold notice, consider appending it to and referencing it in the hold notice.
- Inform custodians of their obligation to preserve electronic and hardcopy documents (including notes, journal entries, post-its, etc.). Emphasize email, instant messages, and text messages (if applicable).

- Consider language clarifying that the company requires full cooperation of all employees in the process and that failure to comply may result in adverse consequences for the company and the employee.
- Consider whether the litigation hold notice must be communicated to relevant witnesses who are no longer at the company.
- Consider asking every recipient to acknowledge receipt and compliance with the hold notice. (Keep in mind that these acknowledgments will evidence the breadth and timing of custodians' compliance.)
- Set up a schedule for regularly reminding recipients of the hold notice of their preservation obligations.
- Update the document preservation instructions if the scope of the investigation changes.

Step Four: *Consider Engaging a Computer Forensics Expert.* The person(s) directing the investigation should decide whether it is necessary to retain a reputable forensic expert or e discovery vendor to capture, host, and possibly help analyze electronic data.

Retention of a computer forensics expert or other e-discovery vendor depends on a variety of variables including:

- Number of custodians or expected volume of raw data
- Need to process and review archived data
- Anticipated productions or external distribution of documents
- Risk of spoliation by relevant custodians
- Identity of reviewers (in-house counsel vs. outside counsel)

If a forensic expert or vendor is engaged, the expert or vendor should be hired by and work under the direction of attorneys so that the attorney-client privilege and work product protection are preserved. The relationship to counsel should be documented in the expert's or vendor's engagement letter.

X. DOCUMENT COLLECTION INTERVIEWS

After the litigation hold notice has been distributed, counsel should conduct preliminary interviews with key document custodians to understand where data related to those facts may exist, how the data is organized, and which other individuals may have knowledge of the matter.

In most instances, you should give interviewees the *Upjohn* warning at the beginning of the interview, just as you would at a substantive interview. For a discussion of the *Upjohn* warning, see Section XIII, *infra*.

Ask the interviewee about his or her personal document practices, including the following:

- Email
    - Filing or archiving and deletion practices
    - Use of various email addresses (work, personal, etc.)
    - Preferred mobile device (smartphones, tablets, etc.)
- Other types of documents frequently used or created
- Method for saving electronic files and locations used (centralized document system, network folders, local hard drive, personal laptop, internet or cloud storage, etc.)
- Personal calendar
- Phone records
- Hardcopy files
- Materials generated and saved at home (including on home computers) or on personal hardware (smartphones, etc.)

Confirm that the interviewee has received the litigation hold notice and is complying with it.

Arrange to collect and secure any potentially relevant or responsive hardcopy documents. Consider who should search for and identify potentially responsive hardcopy documents. In some instances, the custodian may identify hardcopy documents, while in others the outside counsel should conduct the search for hardcopy documents. The documents should be copied and returned to the interviewee. Keep detailed records of what was collected from each custodian.

This is not a substantive interview, but it is an opportunity to gather some preliminary information about the custodians and their roles in the matter under investigation. The impressions and information gathered during the document collection interviews may help determine the need for and order of subsequent substantive interviews.

XI. DOCUMENT REVIEW

In most cases, it will be preferable to complete at least a portion of the document review before beginning substantive interviews. The factual information developed through the review will help make the interviews more effective. Where the volume of documents is high and completing the review before interviews begin is not feasible, consider how to divide the review into phases or otherwise prioritize the review batches.

Step One: *Process the Documents.* Determine the volume of documents collected and decide who will process them.

Generally speaking, high volumes of documents call for an outside vendor.

Efforts should be made to target the most fruitful sources to process in order to reduce the significant cost of processing. Also consider appropriate methods of de-duplication, including email thread suppression and other cost- and time-saving features.

Carefully consider whether and to what extent to restore back-up tapes, which can be very costly. An outside vendor will likely be needed to restore and host the data, and to run the searches necessary to find the potentially relevant records.

Step Two: *Decide Whether to Use Technology Assisted Review ("TAR").* Today's document review software platforms offer TAR—a technology designed to help lawyers identify potentially responsive and privileged documents. This technology generally relies on machine learning and other search algorithms to recognize relevant documents. Typically, a TAR review begins with a relatively small sample (or series of samples) of statistically significant documents. One or two attorneys familiar with the issues in the investigation review and code the documents. The software automates the lawyers' decisions and attempts to apply them throughout the document universe. Results should then be validated through quality control checks of statistically significant samples. Data shows that TAR tools can be impressively accurate and save time and money. TAR can quickly and efficiently identify the most significant documents for an internal review and can also serve as first-level review for production purposes.

Utilizing a provider with TAR capabilities (most providers offer some verison of TAR) may minimize risks and accelerate the timeliness of a review; however, it likely will have a high fixed cost before any documents are processed and is not appropriate in every case.

If documents are being produced to the government, consider conferring with the government before using TAR. Also review any guidance that the government agency has published about the use of TAR and other analytical tools when responding to its requests. Documents may still need to be reviewed manually to confirm responsiveness, privilege, and confidentiality prior to production. Still, using software tools, it is possible to streamline document review to help reduce the time and cost associated with it.

There are innumerable e-discovery or document review platforms. Sometimes more sophisticated tools will reduce review time, but not every investigation calls for a tool with all the bells and whistles. What type of technology is used should be guided by the volume of data to be reviewed and the needs of the particular investigation.

Step Three: *Cull Data.* Various methods can be used to cull the data, including search terms, date restrictions, de-duplication, and removal of irrelevant file types.

Consider working with the IT Department or the outside vendor to develop a list of search terms. This may be a crucial step in the process and should not be shortchanged. (Note, though, this step may be unnecessary or greatly reduced if automated review is used.) Since the advent of "big data" and the growing prominence of information retrieval science, courts and government agencies have become increasingly skeptical of a lawyer's ability to develop effective Boolean queries without expert assistance. It may be advisable to involve search experts, including linguists and information retrieval specialists, to bolster the credibility of the search process. Scientifically-sound search term validation or other quality assurance processes may be needed to ensure that the search terms are meeting acceptable standards of accuracy, are capturing the relevant universe, and are neither returning too many false positives nor missing relevant documents.

It often helps to gather search terms from a narrow set of documents known to be relevant. Glean terms from hardcopy files collected during a document collection interview, for example.

Counsel should consider soliciting input from key employees to help identify common jargon or abbreviations used.

If the government is already aware of the investigation, consider negotiating the process, including search terms used.

Document the culling decisions made, to avoid later second-guessing.

Step Four: *Decide on Reviewers.* This is a key cost control variable.

Options for reviewers usually include in-house counsel, outside counsel (associates), or special project or contract attorneys. Factors to consider include document volume, in-house capacity, billing rates, and the complexity of the legal and factual issues at hand.

Step Five: *Develop a Review Protocol.* Counsel should make sure to spend some time training the document reviewers. The more the review team is integrated into the strategy of the investigation, the better their results will be. Reviewers must be given enough background on the investigation to understand how to spot and tag relevant documents.

Consider whether a memorandum to reviewers explaining the matter and tagging procedures is necessary.

Even if no formal memorandum is drafted, there should be a clearly defined process for escalating questions and disseminating answers, so that documents are tagged consistently by different reviewers.

There should be ongoing quality control and quality assurance with respect to the review. Second- and third-level reviews by more senior attorneys may be necessary depending on time and budget constraints. The more counsel is able to train and trust the first-level review team, the less need there is for re-review of documents.

If disclosure of documents to a regulator or other party is contemplated, it may be prudent to avoid using tags such as "HOT DOC." Consider more neutral, but still accurate, labels.

Step Six: *Keep Track of Key Documents.* As the review progresses, counsel should develop and maintain a working set of key documents to be used in interviews, fact chronologies, etc.

Although tags in the document review platform are useful, at some point, it often makes sense to put the core set of key documents in binders or on a flash drive for review by those in charge of the investigation. It also may be useful to apply an internal bates stamp to these documents for easy reference and tracking.

Counsel's and client's conduct in preserving and producing electronic records are increasingly subject to scrutiny and second-guessing by regulators, courts, and other third parties. Applicable standards of care are evolving and often require the expertise of e-discovery vendors, consultants, or counsel. Make good faith efforts to confirm the process followed is defensible given current trends. Document the process to support its reasonableness and diligence. Key items to document include:

- The litigation hold notice, process used to identify recipients, list of people who received the notice, the dates the notice and reminders were sent, and confirmations that the notice was received
- Custodian list
- Data collected from custodians and centralized sources
- Volume and cost of retrieving data; including sources deemed not reasonably accessible due to the technology involved or the cost to retrieve and/or review the data
- Culling procedures and validation and quality control measures used
- Custody or control issues regarding data from former employees, affiliated companies, and other third parties

XII. PREPARING FOR INTERVIEWS

Step One: *Determine Persons to Be Interviewed.* Start compiling a list of interviewees. The custodian list created at the beginning of the investigation is often a good place to start, especially if the list has been updated as the document review has progressed.

- Information may have emerged during the document collection or review process that indicates that a person thought to have relevant information actually does not.
- Conversely, facts may have emerged pointing to other individuals who should be interviewed.

Consider interviewing third parties with relevant information and employees or former employees who are not document custodians but are referenced in key documents. These interviews can yield valuable information that may not be otherwise obtainable through document collection and review. Generally, third parties have no duty to cooperate with the company, but they may nonetheless consent to an interview. Determine if former employees have a contractual commitment to cooperate in internal investigations as part of any severance agreement or employment contract.

Be aware, however, that interviews with former employees and third parties may not be protected by the attorney-client privilege, and, in the absence of a non-disclosure agreement, may not even be confidential. Counsel should make the judgment call ahead of time whether the potential information to be gained through the interviews outweighs the potential disclosure risk of conducting interviews without the protection of privilege. Factors to consider in this decision include the following:

- Communications with former employees about events that occurred within the scope of their prior employment may be subject to the attorney-client privilege.
- Employees who left the company under adverse circumstances may be more likely to divulge confidential information from the interview. In the absence of a contractual provision obligating a former employee to cooperate in an investigation and maintain confidentiality, a company may not have effective remedies against a former employee who breaches confidentiality. Such contractual provisions cannot be used to prevent a whistleblower from reporting information to a government agency.
- Attorney-client privilege may cover consultants considered the "functional equivalent" of corporate employees.
- Outside counsel may ultimately be called to testify as witnesses in government investigations and/or proceedings regarding non-privileged interviews of third parties conducted by outside counsel.

Determine the appropriate sequence of interviews, which is often a strategic matter. Modify as appropriate as the investigation unfolds. This strategy decision may be impacted by such concerns as listed below:

- Background scoping interviews typically occur early in the investigation and are primarily aimed at uncovering sources and locations of relevant information, as well as the nature and extent of the witness's knowledge. Scoping interviews may also provide an overview of corporate processes, practices, and personnel. Substantive interviews should normally be conducted after the relevant documents have been reviewed where circumstances allow. Some witnesses may need to be interviewed again.

- Adjust the timing of the interviews so as to best position the company for cooperation. If witnesses may terminate employment, or consultants' contracts may terminate, during the course of the investigation, conduct the interview while the witness is still employed or under contract. Also consider other circumstances beyond the facts of investigation that may have an impact on sequence, such as upcoming retirements or long-term foreign travel.

- It may make sense to gather information from lower-level employees first so that the information can be used in later interviews with key or higher-level witnesses. It is generally prudent to save highest priority interviews for later, after important facts are developed and documents are reviewed, so that counsel is better equipped to ask informed questions. On the other hand, interviewing the key witness first is sometimes a sound strategy if there is a risk that the witness will learn about the format and substance of the first interviews and then tailor his or her statements accordingly.

- Consider concurrent interviews if collusion among witnesses is a concern.

- Employees who are, or may become, whistleblowers may merit special consideration. Promptly interviewing a whistleblower may help define the scope of the investigation. An early interview may also earn the whistleblower's trust and serve to postpone reporting outside the company. Be aware, though, that what is said or done in the interview will likely be reported, along with the underlying allegations. See Section VII, supra, for additional special considerations regarding whistleblowers.

Step Two: *Schedule the Interviews.* Do not underestimate the amount of time it will take to calendar all of the interviews. It may be difficult to secure time on a witness's schedule, particularly with respect to directors or executives.

Create a master calendar for the interviews, indicating locations and who will be present.

On the interviewer side, there should always be two attorneys present.

- One attorney asks questions, while the other takes notes.

- The note taker should fully document the warnings given to the witness rather than providing a summary statement such as "*Upjohn* warning given."

- Both attorneys should be familiar with the documents and other interviews in the investigation.

Attorney notes are preferable to an audio or video recording of an interview because the notes are more likely to be protected from disclosure by the work product doctrine. Recordings are potentially discoverable by third parties. If an employee requests that his or her interview be recorded, consult senior legal personnel or outside counsel before consenting.

If the investigation is being conducted by outside counsel, in-house counsel ordinarily should not attend interviews. Depending on the circumstances, the presence of in-house counsel may jeopardize the perceived independence of the investigation. On the other hand, there may be situations where having in-house counsel present will be helpful, such as where the investigation centers on a technical component of the company's business and outside counsel is not versed in the company's terminology.

Interviews should ordinarily be conducted in person, rather than by telephone or video conference. Veracity, cooperation, demeanor, and body language are often difficult to assess when not face-to-face with the witness. Establishing rapport with the interviewee and effective note-taking can also be challenging when done remotely. Interviews in which documents will be reviewed are particularly cumbersome to conduct remotely.

Consider where to conduct interviews, with the goal of finding a neutral, private, and convenient place that will allow the witness to speak openly. Although it is laudable to try to avoid business disruption, employees may be more forthcoming when interviews are conducted off-site.

Attorneys with investigation experience should conduct the interviews, especially the interviews of key or high-level witnesses.

There are advantages to having the same attorney or attorneys interview persons with knowledge of the same aspect of the subject of inquiry.

On the interviewee side, the company can generally insist that its employees participate in internal investigation interviews.

- If employees are unionized, it may be necessary to work through union representatives. The employee may have the right to have a union representative present at the interview if questioning could lead to disciplinary action (so-called *Weingarten* rights[19]). If a union representative is present, a court could find that the interview is not privileged.[20] The union's bargaining agreement may also provide an employee with a right to representation.
- If employees indicate that they do not wish to participate in an interview or otherwise cooperate, remind them of any company policies that require cooperation with investigations and tell them immediately that they will likely be subject to discipline if they refuse to be interviewed. If they continue to resist, in-house counsel should consult with

[19] Named after the case *NLRB v. Weingarten, Inc.*, 420 U.S. 251 (1975).
[20] *See, e.g., Wong v. Bd. of Educ. of Cmty. Consol.*, No. 11-CV-07357, 2013 WL 6571326, at *2 (N.D. Ill. Sept. 30, 2013) ("No controlling authority establishes a federal privilege protecting employee-union representative communications.").

outside employment counsel before taking disciplinary action. Special considerations apply to whistleblowers in this regard.

- The duty to participate includes an obligation to be truthful and cooperative in all aspects of the investigation.

Consider and anticipate whether particular employees have contractual rights or legal rights such as a right to privacy, whistleblower rights, rights under the Fair Credit Reporting Act, or union-related rights.

- A blanket rule prohibiting unionized employees from discussing an ongoing internal investigation may violate the National Labor Relations Act; instead, the company may need to show that it has a legitimate business justification for requiring confidentiality.[21]

- Take special care if interviewing a whistleblower. Whistleblowers present unique risks of retaliation claims or allegations that the company did not conduct a proper investigation. Avoid warnings of discharge or other action that may appear retaliatory until those options are fully assessed with outside employment counsel. In the interview, counsel should avoid any appearance that the interview is punitive, threatening, or coercive. Make and record a non-retaliation pledge. Another member of the investigative team should be present at the interview to take copious notes and act as a witness in case a whistleblower subsequently challenges how the interview or investigation was conducted.

- Interviews of high-ranking executives should also be handled with care. These witnesses may be entitled to advancement or indemnification provisions under the company's charter or bylaws. It may be advisable for these witnesses to obtain separate counsel so that they will be better prepared and less likely to make inaccurate statements in their interviews.

Step Three: *Consider Counsel for Witnesses and Providing Documents to Witnesses.*

Allowing employees to have their personal attorneys present at an interview may result in witnesses being less forthcoming or declining to be interviewed at all. Nevertheless, in some situations, it may be preferable to have separate counsel present.

- For a discussion of whether individuals within the scope of the investigation need separate counsel, see Section IV, *supra*.

- For a discussion of what to do if an employee asks whether he or she needs counsel at the interview, see Section XIII, *infra*.

In preparing for the interviews, counsel should identify and select which documents will be referenced. Reviewing documents in advance informs the interviewer, allows for more detailed questioning and probing of inconsistencies, and helps avoid multiple rounds of interviews.

[21] *Banner Health Sys. d/b/a/ Banner Estrella Med. Ctr.*, 358 N.L.R.B. No. 93 (July 30, 2012).

Whether documents should be provided to the witness before the interview may vary depending on the nature and circumstances of the investigation.

- Documents may not be provided in advance if there are concerns about witness tampering or obstruction of justice, or if the company is the victim of the conduct being investigated.
- Providing documents in advance can speed up the actual interview by refreshing the witnesses's recollections.
- Not providing documents in advance may make the interview feel more adversarial and may lead to unintentionally inaccurate statements by the witness that are against the company's interest.

If documents are provided to witnesses before interviews, consider maintaining a master list of exhibits for all witnesses or a separate Bates range to track documents shared with witnesses.

Consider obtaining background information about the witness through the company's personnel files, internet searches, and publicly accessible databases. In certain cases, it may be important to have an understanding of the witness's job performance, prior employment experiences, financial information, criminal or litigation history. Keep in mind, though, that federal, state, and local laws regulate an employer's obtaining and/or using background information on employees.

Step Four: *Prepare an Interview Outline.* All interview outlines should be drafted with the objectives of the interview in mind.

There may be any number of objectives for an interview, including discovering facts, locking in statements or preserving evidence, assessing witness credibility, protecting attorney-client privilege and work product, and enhancing the credibility of the investigation.

Generally speaking, interviews are most effective when the interviewer asks a mix of general questions and specific questions based on documents.

Be prepared to deviate from your outline; follow up on answers given.

It is often useful for the attorney conducting the interview to utilize an interview binder that contains a detailed interview outline, relevant documents (with key portions highlighted), prior witness statements, relevant statements of other witnesses, an organizational chart, and background materials on the witness.

- This binder should not be shown to the witness or the witness's counsel.
- Documents shown to the witness should not contain any highlighting, and should not include any privileged information or work product.
- The note taker at the interview should keep track of documents used and specifically reference them in the interview memorandum.

Step One: *Give the Appropriate Warnings.* Begin every interview by explaining who you represent and the basic parameters of the investigation. A best practice for most interviews is to give an *Upjohn* warning[22] similar to the sample warning below. In some jurisdictions, the rules of professional responsibility impose a duty on attorneys representing corporations to explain the identity of the client to the corporation's directors, officers, employees, or other associated persons when it is apparent that the corporation's interests may be adverse to the persons with whom the lawyer is dealing.[23] Lawyers conducting internal investigations should familiarize themselves with any such rules applicable to them.

Sample *Upjohn* Warning:

> "I am a lawyer for [Company Name or Board Committee]. I represent only the company. I do not represent you personally. I am conducting this interview to gather facts in order to provide legal advice for [Company Name or Board Committee]. Your communications with me are protected by the attorney-client privilege, but the attorney-client privilege belongs solely to [Company Name or Board Committee], not you. That means that the [Company Name or Board Committee] alone, and at its discretion, may elect to waive the attorney-client privilege and reveal our discussions to third parties. The company does not need your consent to make such a disclosure. In order for this discussion to be subject to the privilege, it must be kept confidential. In other words, with the exception of your own attorney, you may not disclose the substance of this interview to other employees or anyone outside of the company. Do you have any questions?"

It ordinarily is not necessary to give this warning in writing, although doing so may be prudent if there is reason to think that the witness will deny having received the warning.

In giving the *Upjohn* warning, and during the interview in general, adopt a fair-minded, courteous and objective tone. Remember that employees are likely to be nervous. Do not create an intimidating or hostile atmosphere.

An *Upjohn* warning may not be appropriate or necessary in all instances, and may unnecessarily alarm those who are being asked to provide only background or technical assistance and are clearly not in harm's way. Great care should be taken, however, in determining that an *Upjohn* warning is not necessary. Consider the following in determining whether to give an *Upjohn* warning:

- Is there an apparent conflict of interest between the company and the witness?
- Is the witness a whistleblower?
- Is the witness an employee or a third-party consultant who may be deemed the functional equivalent of an employee?

[22] The name of the warning derives from the Supreme Court's decision in *Upjohn Co. v. United States*, 449 U.S. 383 (1981). In *Upjohn*, the Court held that a corporation's attorney-client privilege could cover communications between company lawyers and non-management employees.
[23] *See, e.g.*, District of Columbia Rules of Professional Conduct, Rule 1.3. Rules such as these typically are based on the ABA Model Rules of Professional Conduct, Rule 1.13(f).

- Is the witness a former employee who will be interviewed about his or her conduct and knowledge gained during employment?
- Is the witness an executive who may believe or claim to believe that the company's counsel is his or her own, potentially giving rise to an implied attorney-client relationship?

Inadequate *Upjohn* warnings may jeopardize the privileged nature of the interview, affect the company's ability to report the interview results to a government entity or third party, subject the attorney to criticism or discipline, and may impede the company's cooperation with the government.

Counsel should receive a clear affirmation that the witness understands the warning and is willing to proceed with the interview.

Remind witnesses that they have an obligation to tell the truth.

- In some circumstances, such as when disclosure to the government is probable, it may make sense to give a *Zar* warning.[24] The *Zar* warning tells employees that information provided during the interview may be turned over to the government. A *Zar* warning should not be given without careful consideration and consultation with outside counsel.

If employees being interviewed ask whether they need a lawyer, ordinarily you should respond that you cannot give them advice on that matter and that they need to make that decision themselves.

- Depending on corporate articles of incorporation or bylaws and indemnification agreements, the company may be obligated to pay the employee's attorneys' fees. Depending on the situation, you may want to offer to provide the employee with a personal attorney at company expense. Be aware of company policies, bylaws, and contractual provisions prior to the interview.
- If key witnesses are able to consult with an attorney, they are more likely to be accurate in what they say and less likely to invent a story that turns out to be untrue.
- Never advise an employee to assert the Fifth Amendment to a government agent. In certain circumstances, this instruction could be construed as obstruction of justice.

Employees may ask whether they will be fired or disciplined if they refuse to answer. Make sure you know the legal rules and company policies before going into the interview. Some state statutes provide that every employee owes a duty to cooperate to his or her employer. Most

[24] In *United States v. Zar*, Cr. No. 04-331 (E.D.N.Y. 2004), a former executive of Computer Associates, Inc. pleaded guilty to charges of obstruction of justice based on statements made to the company's outside counsel conducting an internal investigation. *See also United States v. Kumar & Richards*, Cr. No. 04-847 (E.D.N.Y. 2004). *Zar* and *Kumar* are sometimes referred to as the *Computer Associates* cases. The Second Circuit ultimately affirmed the result in *Kumar*, though without ruling on the merits of whether statements to outside counsel could serve as the basis for an obstruction charge. *See United States v. Kumar*, 617 F.3d 612, 619–20 (2d Cir. 2010).

company codes of conduct and employee manuals also impose a duty to cooperate. Refusal to cooperate can result in disciplinary action, including loss of employment.

If employees ask if the interview can be conducted "off the record," explain that an "off the record" approach is inconsistent with your obligation to document all material facts.

Step Two: *Ask Clear, Open-Ended Questions.*

Interviews typically begin with background questions to help establish an interview rhythm. Move to more specific questions and documents when a rapport has been established.

Always treat witnesses respectfully. An overly adversarial approach reduces the likelihood that the witness will be open and is bad for employee morale.

Generally, you should not convey information to witnesses during the interviews. The witness, not the attorney, should be the one supplying the information. Similarly, avoid framing questions in a way that suggests an answer or a course of conduct. Remember:

- Asking questions in a way that influences a witness's answers may later be viewed as witness tampering.
- Be careful not to potentially influence the witness's account by sharing details of another witness's account.

Use the interview outline to make sure you cover all pertinent topics.

Use the interview as an opportunity to gather leads to other witnesses and documents. Ask questions such as: "Who might know more about that? What kind of documents could I look at to find that out?"

You may also be able to probe a witness's bias and motive during the interview.

Be persistent without being adversarial. Follow up on a witness's answers. Make sure that you get the information you seek without unnecessarily intimidating the witness. A good rule of thumb is to assume that someone—you, your colleague, and/or the witness—will testify one day about what happened at the interview.

For possibly culpable witnesses or witnesses who appear to be lying: anticipate and be prepared to confront them with contrary evidence. Consider whether you want to ask open-ended questions first, or try to preempt any falsehood by providing documents and asking leading questions.

Conclude with catchall questions as appropriate—"Is there anything else I should know?"; "Is there anything else you would like to tell me?"

Step Three: *Close the Interview.*

Advise employees to keep the contents of the interview confidential. This warning is necessary to preserve the company's privilege.

Remind employees not to discuss the subject matter of the investigation with anyone other than their attorney (if applicable). This prohibition extends to emails as well as oral conversations.

Remind employees of their document preservation obligations.

Advise employees that they may be interviewed again, in which case they will be asked about any communications they had with anyone between the two interviews regarding the subject matter of the investigation.

Consider whether to advise employees that they may be contacted by government investigators and to request that employees promptly advise the company of any such contacts or communications. Do not advise or encourage the employee not to speak with the government investigator, which may create liability risk under witness tampering and obstruction of justice statutes. The company may decide to distribute a written notice to all relevant employees describing the employees' rights if they are contacted by government agents. (*See* Appendix B.) Consult with counsel to ensure that the notification is carefully drafted, balanced, and fair.

Tell the employees to reach out through a designated contact if they recall additional information or seek to make a clarification.

Step Four: *Document the Interview.*

The person who took the notes should generally author an interview memorandum that begins with an introductory paragraph making it clear that the memorandum is protected by the attorney-client privilege and the work product protection.

The interview memorandum ordinarily should not be a verbatim account of what was said at the interview, but instead contain counsel's mental impressions, opinions, subjective analyses, and conclusions concerning the interview. Using a transcript format or otherwise avoiding reorganization and analysis may increase the chances of losing work product protection, but may be more effective if the memorandum will likely be used to impeach a witness.

The interview memorandum should contain the following:

- The date the memorandum was drafted
- The names of all individuals present at the interview
- The date and location of the interview
- A clear description of the warnings given to the witness, including the Upjohn warning and the closing comments
- An accurate record of what the witness said, presented in a narrative fashion, with references and relevant quotes to exhibits shown to the witness
- A description of significant non-testimonial events such as the fact that the witness stepped outside to make a phone call, the witness's demeanor, etc.

Avoid characterizations or conclusory statements. If in doubt about what the witness said, confer with the other attorney who was present or ask the witness to confirm.

Prepare the interview memorandum while the interview is still fresh in your memory.

Only one interview memorandum should be created. Avoid creating multiple versions of the document.

After the interview memorandum is drafted, the other attorney present should review the memorandum to confirm its accuracy before it is finalized.

XIV. CREATING RECORDS AND REPORTS DURING AN ONGOING INVESTIGATION

A. Periodic Updates

While document review and interviews are ongoing, counsel leading the investigation should provide regular updates to the person(s) directing the investigation. Where there is a risk that the investigative record will be produced in subsequent litigation or where there is a possibility of disclosure to the government, it is generally preferable to provide the updates orally. So long as the investigation is ongoing, interim conclusions are susceptible to revision. Prematurely recorded and inaccurate information could subsequently be used against the company or individual witnesses.

Make clear to your client that periodic reports are made in real time, your understanding of facts will evolve over the course of the investigation, and a conclusion that appears correct at one point may prove to be incorrect after more information is learned. It is important, therefore, to be conservative in reaching conclusions before the investigation is complete.

Records of the oral reports may be kept in the form of meeting minutes that are clearly marked attorney-client privileged and attorney work product. The minutes should be detailed enough to demonstrate that the person(s) directing the investigation were kept apprised of important legal and factual issues, but not so detailed as to create the problem described above.

B. Other Attorney Work Product

Any documents counsel creates during the course of the investigation—chronologies, memoranda, summaries, etc.—should be labeled as “attorney work product” and kept in a secure, centralized location. Where a subsequent production of evidence is contemplated, it is important that counsel maintain detailed records of document collection and processing.

XV. DETERMINING REMEDIATION

Failure to adopt remedial steps if the investigation uncovered misconduct or deficient internal controls may expose the company, individual officers, or directors to additional liability. Prompt action to implement remedial measures can bolster a company's arguments regarding its good-faith efforts.

Step One: *Halt All Improper Conduct.* A first step is immediately stopping any misconduct uncovered by the investigation.

Regulators and prosecutors will not look favorably on any delay.

Step Two: *Consider Disciplining Wrongdoers.* Next, the company may need to consider disciplining responsible employees. Factors that should be considered are:

- Seriousness of the misconduct
- Need to deter future misconduct
- Business needs of the company
- Risk of appearance of scapegoating
- Consistent treatment across employees, i.e., no disparate treatment of higher- and lower-level employees, or employees with protected characteristics (e.g., race, gender, age, religion, disability, etc.)
- Potential whistleblower concerns (see Section VII, *supra*)

Note that in some jurisdictions, employees who are disciplined may be entitled to information about the investigations on which the adverse employment action was based, regardless of whether it was a privileged investigation.

- If an employer takes an adverse action based on a third-party investigation into alleged employee misconduct or noncompliance with laws, rules, regulations, or policies, the federal Fair Credit Reporting Act requires that the employer provide the employee with a summary of the "nature and substance" of the investigation. The summary need not be written or identify the sources of information contained in the report.
- If the employer seeks to use an internal investigation to defend itself in subsequent litigation with the employee, it will ordinarily be required to waive the privilege.[25]
- The company may be required to disclose information obtained from the investigation, including witness statements, to a union if the union requests them for grievance or arbitration purposes.[26]

[25] *See Wellpoint Health Networks, Inc. v. Superior Court*, 59 Cal. App. 4th 110, 125-28 (1997); *Kaiser Found. Hosps. v. Superior Court*, 66 Cal. App. 4th 1217, 1223-28 (1998).
[26] *Am. Baptist Homes of the W. d/b/a Piedmont Gardens*, 359 N.L.R.B. No. 46 (Dec. 15, 2012).

Premature disciplinary actions before all the facts have been gathered may impede the investigation and also expose the company to potential defamation or wrongful termination claims.

If a whistleblower is implicated in the misconduct, whistleblower protections may limit the company's ability to lawfully terminate or discipline these individuals.

In determining the appropriate discipline and the procedures to follow, consult with employment counsel and human resources. Objections to discipline from an employment law perspective must be balanced against the consequences of not being able to show a regulator a record of swift and complete action. Also consider whether continued cooperation is needed from an employee in order to adequately uncover facts and cooperate with the government; a disciplined employee may be reticent to continue cooperating. Coordination will allow for a balanced decision considering all of the circumstances and consequences.

Step Three: *Consider Other Potential Remediation.* Other potential remedial measures may include the following:

- Establishing or enhancing compliance controls, procedures, and/or training to help prevent recurrence of the same problems in the future.
- Compensating injured third parties (if identifiable).
- Returning erroneously paid government funds.

Step Four: *Formulate a Plan for Implementation.* Once the person(s) overseeing the investigation has determined appropriate remediation, develop a work plan and timeline for rolling out all remedial measures, designate personnel responsible for execution, and create a mechanism for monitoring remediation efforts to ensure they are effectively implemented. Doing so ensures appropriate follow-through and serves to document the concrete results of the investigation.

XVI. REPORTING THE RESULTS OF AN INTERNAL INVESTIGATION

At the conclusion of the investigation, it is usually necessary and appropriate to give some type of report to the person or group that authorized the investigation.

A. Written or Oral Report?

An important question is whether the final report should be oral or in writing. There are a variety of risks associated with written reports, including the following:

- Ordinarily, a written report is significantly more expensive than an oral report.
- The contents of the report may be used against the company in parallel civil proceedings. In some cases, statements in the report may be construed as admissions.
- A written report will contain much more detail that can be subject to second-guessing.
- Providing the written report to the government may result in a broad waiver of privilege, opening up the investigative files to discovery, even if produced to the government under a confidentiality agreement.

In light of these risks, the convention is to provide an oral report where possible. Oral reports minimize (but may not completely alleviate) the risks of discovery of the report and preserve the company's flexibility going forward. Where an oral report is given, the size of the audience should be carefully limited. An attorney should take minutes of the meeting, include a list of all attendees, and document that appropriate privilege and work product warnings were given at the outset of the meeting.

There are some situations where a written report will be necessary. For example:

- A government agency may demand it.
- In a derivative action, the report may be the basis for a motion to terminate the litigation.
- If the underlying factual circumstances are complex, a written report may be a valuable persuasive tool in dealing with the government and other adversaries.
- A written report may be helpful to document that the directors overseeing the investigation have fulfilled their fiduciary duties.
- A written report may be helpful to document employment discipline determinations.

Written reports must be prepared with great care. Counsel should clearly distinguish between facts and opinions and draw only those conclusions that are warranted by the facts. Supporting evidence should be verified before publication, and drafters should avoid colorful language.

The report should be labeled "Privileged & Confidential – Attorney-Client Communication – Attorney Work Product."

The report should contain a succinct statement of the purpose of the investigation and a description of the scope and procedures followed.

Any assumptions made should be stated explicitly.

Where the investigation uncovered conflicting evidence (documents, witness statements, etc.), discrepancies should be noted. Any assessments of credibility, if included at all, should be cast as opinion and be accompanied with reasoned justifications.

As with an oral report, the company should limit distribution of a written report. It is often advisable to keep a log of recipients, set a time limit for review and then retrieve all copies.

The company should maintain written reports in privileged and confidential files.

Counsel preparing the report should be aware of the risk of a defamation lawsuit brought by individuals who are not depicted favorably in the report. Some situations may even warrant a conversation between counsel and the company regarding indemnification against claims based on the content of the report.

A frequently used middle ground between an oral report and a written report is an oral report supplemented by a PowerPoint presentation that highlights key points, but does not contain as much detail as a written report.

B. Who Gets the Report?

Whether oral or written, consider carefully who gets the report. Individuals and entities who receive the report may include a combination of the following:

- The client of the counsel preparing the report
- The Board and/or certain Board committees
- Management
- Auditors
- Insurers
- Government or regulators
- Whistleblowers, if any

Privilege law surrounding intra-company disclosures is unsettled. Only the client enjoys privilege. If disclosures are made outside the attorney-client relationship or under a common interest agreement, a waiver may occur. For example, sharing privileged information about the investigation with non-committee members of the Board can constitute a waiver if they have been implicated in the allegations giving rise to the investigation.[27]

[27] *See Ryan v. Gifford*, No. 2213-CC, 2007 WL 4259557 (Del. Ch. Nov. 30, 2007) (finding that the special committee conducting the internal investigation waived privilege by disclosing its communications concerning the investigation and its final report to directors named as defendants in the derivative suit and their counsel).

XVII. NOTIFYING THE GOVERNMENT AND PUBLIC DISCLOSURE

An issue that may arise at the conclusion of an internal investigation is whether to disclose the findings to prosecutors, to a regulator, or in an SEC filing.

Disclosure is mandatory in a few circumstances, and the reporting requirements of the Federal Acquisition Regulation Act ("FAR"), Sarbanes-Oxley Act, the Anti-Kickback Act, Comprehensive Environmental Response, Compensation, and Liability Act, and the Clean Water Act should all be considered, as should any potentially applicable statutes or regulations, government contracts, and administrative agreements.

If the results of the investigation would be material to investors, the company's disclosure counsel should be consulted. SEC Rule 10b-5 may require disclosures where necessary to correct a previously misleading public disclosure.

In other circumstances, voluntary disclosure will depend on a number of different factors, including:

- The likelihood that the government will learn about the issue, whether through a whistleblower, a competitor, or otherwise, even if the company does not voluntarily disclose. If the government is going to find out anyway, it ordinarily is better to voluntarily disclose.
- The severity of the conduct and the nature of the remedial action undertaken. If the misconduct was limited to low-level personnel, was not pervasive, and sufficient remedies were undertaken as a result of the investigation, the company may choose to take a "wait and see" approach.
- Whether the company is willing to disclose to the government all individuals potentially involved in any wrongdoing and to completely disclose all "relevant facts." Failure to do so could negate any credit (e.g., a lesser penalty for the conduct) given in exchange for the company's disclosure and cooperation with the government.[28]
- The likelihood of obtaining a non-prosecution decision, a reduced charge, or other favorable outcome on the basis of voluntary disclosure. This assessment must be made on a case-by-case basis, considering the particular government agency and official to whom the disclosure will be made, any delay between discovery and disclosure, and the type of allegations and severity of conduct. [29]
- The potential that cooperation will reduce the company's culpability score under the Federal Sentencing Guidelines. Chapter Eight of the Guidelines contains the framework for sentencing corporations.

[28] *See* Sally Q. Yates, Memorandum, *Individual Accountability for Corporate Wrongdoing* (Sept. 9, 2015), *available at* https://www.justice.gov/dag/file/769036/download; Sally Q. Yates, *Remarks at New York University Law School Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing* (Sept. 10, 2015), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

[29] Companies generally need not worry that deferred prosecution agreements (and non-prosecution agreements) entered into with the government will be rejected by the judiciary, reopening the question of prosecution despite having arrived at a favorable agreement post-cooperation. *See United States v. Fokker Servs.* B.V., No. 15-3016, __ F.3d __, 2016 WL 1319266 (D.C. Cir. Apr. 5, 2016).

- The benefits of solidifying the company's relationship with the government. In a situation where the government is conducting an industry-wide probe, for example, there may be advantages to differentiating the company through cooperation.
- The risk that the disclosure will prompt the government to investigate conduct that was otherwise not on its radar screen.
- The potential burdens of cooperation. The government may look to the company's outside counsel for legal analysis and factual development. The investigation may expand into other areas. Self-reporting is not a simple process, and most government entities will expect corporate counsel to stay involved and help manage further investigation, including document production. This can be very costly.
- The potential collateral consequences of disclosure. Self-reporting to the government may prompt parallel civil suits and prosecution of individual employees.
- The scrutiny to which the internal investigation itself will be subject following disclosure.
- The substantive law under which the investigation of wrongdoing occurred, and the associated benefits. For example:
    - In the antitrust area, full criminal amnesty frequently depends on being the first to disclose. If the investigation reveals potential anticompetitive conduct, the company must strongly consider applying for a "marker" from DOJ's Antitrust Division, which temporarily secures its first-in status while the company completes its investigation to "perfect" the leniency application. The marker is in effect for a finite period, typically 30 days, but can be extended. If the internal investigation does not uncover a breach of antitrust laws, the marker may be withdrawn or allowed to lapse. Otherwise, to obtain a conditional leniency letter, the company must demonstrate its willingness to cooperate, provide detailed attorney proffers, documents, and percipient witnesses on the criminal conduct reported, admit to a criminal antitrust violation, and meet other requirements for eligibility. After DOJ's investigation and any ensuing prosecution has concluded and the applicant has satisfied all of its obligations, the Division will issue a final leniency letter.
        - Where applicable, consider applying simultaneously for leniency in multiple jurisdictions.
    - Voluntary disclosure under the FCA or FCPA may help the company argue for lower penalties. For example, the "not less than double damages" provision of the FCA requires that all information known about the violation be reported to the government within 30 days of receiving the information. As another example, DOJ recently announced a one-year "pilot program" offering substantially lower

penalties for companies that voluntarily disclose violations of the FCPA and "fully cooperate" with the government's investigation.[30]

- Voluntary disclosure of violations of export controls and sanctions laws can help mitigate penalties. Although the different agencies involved in the enforcement of export activity generally encourage disclosures, each has different rules and practices. The Office of Foreign Assets Controls ("OFAC") of the U.S. Department of Treasury has the clearest guidelines for penalty mitigation—the base penalty amount is reduced by 50% in cases of voluntary disclosure. Even if the self-disclosure occurs after OFAC or another government agency discovers a violation, the OFAC penalty may still be reduced by 25% to 40% if the violators provide "substantial cooperation."

By the time a company chooses to self-report a potential issue to a government authority, it should already have engaged competent outside counsel with experience dealing with that authority. Self-reporting often spurs a lengthy negotiation process, and the company will want a credible advocate working on its behalf.

Public disclosure may be required if the investigation renders existing disclosures false or misleading. It is important to consult with disclosure counsel to determine if new disclosures are necessary or existing disclosures need to be modified or withdrawn.

If the company decides to disclose, it may want to seek the aid of marketing, public relations, or government relations firms to develop the company's message to shareholders, customers, the media, and even the government. Federal courts are divided over whether communications with public relations consultants are privileged.

[30] *See* Andrew Weissmann, Memorandum, *The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance* (Apr. 5, 2016), *available at* https://www.justice.gov/opa/file/838386/download.

XVIII. SUMMARY OF INTERNAL INVESTIGATION DO'S AND DON'TS

Do's	Don'ts
• Do spend time at the outset defining the goals and scope of the investigation	• Don't focus the inquiry too narrowly
• Do take immediate action to preserve and collect potentially relevant documents	• Don't wait to preserve until after you conduct document collection interviews
• Do create clear protocols up front to govern how the investigatory team retains and shares information and communications, so the attorney-client privilege is protected	• Don't assume that information will remain privileged or confidential just because everyone is "working together"—formalities matter
• Do check if local law will affect international investigations, especially on employment and data privacy issues	• Don't assume that the rules are the same in the United States and in other countries
• Do be mindful of whistleblower issues from the get-go, including anti-retaliation protections	• Don't take any action that might be perceived as retaliatory without first obtaining approval from counsel
• Do develop a document review protocol and tagging system	• Don't use tags like "HOT DOC - BAD"; use more neutral tags
• Do give regular updates to the individuals directing the investigation	• Don't prematurely give or record interim conclusions
• Do label documents "Privileged & Confidential," "Attorney-Client Communication," and "Attorney Work Product"	• Don't use attorney-client privileged documents or attorney work product documents to refresh a witness's recollection during an interview
• Do maintain detailed records of document collection and processing; also track which documents are used in witness interviews	• Don't rely exclusively on the tags in the document review tool; as the investigation progresses, segregate key documents
• Do create a strategy for identifying likely witnesses and taking interviews	• Don't go into interviews "blind" without considering where the witness fits in the overall investigation strategy

Do's	Don'ts
• Do take extra precautions if interviewing whistleblowers or third parties	• Don't assume that interviews of whistleblowers or third parties will remain confidential
• Do give witnesses Upjohn warnings at witness interviews, unless specifically determined to be unnecessary	• Don't, under any circumstances, advise a witness to assert the Fifth Amendment, advise a witness against speaking or cooperating with government or law enforcement, or give advice to a witness regarding whether or not to obtain individual counsel
• Do be persistent and follow up on a witness's answers	• Don't attempt to intimidate witnesses
• Do draft interview memoranda as soon as practicable after the interviews	• Don't create multiple versions of interview memoranda
• Do promptly halt any improper conduct discovered during the investigation	• Don't limit messaging regarding halting improper conduct to too narrow of an audience
• Do carefully consider whether the final report should be oral or written	• Don't draw conclusions that are not clearly warranted by the facts
• Do take appropriate remedial measures at the conclusion of the investigation	• Don't allow remediation to slip through the cracks; develop a means for monitoring progress
• Do discipline wrongdoers	• Don't appear to be retaliating against a whistleblower or passing blame off to low-level employees
• Do consult the attorney leading the investigation or outside counsel when you have questions	• Don't proceed with public disclosure of the results of an investigation without obtaining the advice of outside counsel

XIX. REFERENCES

6 U.S.C. § 1504(d)(1) (Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act 2016, Division N), Pub. L. 114-113, codified at 6 U.S.C. §§ 1501-1510 (CISA)).

Akzo Nobel Chems., Ltd. v. European Comm'n, Case C-550/07 P, Judgment of the Court (ECJ Sept. 14, 2010).

Ambac Assurance Corp. v. Countrywide Home Loans, Inc., 124 A.D.3d 129 (N.Y. App. Div. 2014).

Am. Baptist Homes of the W. d/b/a/ Piedmont Gardens, 359 N.L.R.B. No. 46 (Dec. 15, 2012).

American College of Trial Lawyers, *Recommended Practices for Companies and Their Counsel in Conducting Internal Investigations*, 46 Am. CRIM. L. REV. 73 (2009).

Andrew Weissmann, Memorandum, The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance (Apr. 5, 2016), available at https://www.justice.gov/opa/file/838386/download.

Banner Health Sys. d/b/a/ Banner Estrella Med. Ctr., 358 N.L.R.B. No. 93 (July 30, 2012).

Congressional Research Service, Survey of Federal Whistleblower and Anti-Retaliation Laws (Apr. 22, 2013), *available at* http://fas.org/sgp/crs/misc/R43045.pdf.

Corning Inc. v. SRU Biosystems, LLC, 223 F.R.D. 189 (D. Del. 2004).

DAN K. WEBB, ET AL., CORPORATE INTERNAL INVESTIGATIONS (2009).

Daniel H. Bookin, Sara E. Jeruss & Jean Niehaus, *Maintaining Attorney-Client Privilege and Work Product Protections in Internal Investigations*, in PRACTISING LAW INSTITUTE, INTERNAL INVESTIGATIONS 2009: HOW TO PROTECT YOUR CLIENTS OR COMPANY (PLI 2009).

Daniel H. Bookin, Sharon M. Bunzel & Laurie K. Dean, *Obstruction of Justice Under Computer Associates: Legal, Tactical and Ethical Implications for Attorneys Conducting Internal Investigations, in* PRACTISING LAW INSTITUTE, INTERNAL INVESTIGATIONS: LEGAL, ETHICAL & STRATEGIC ISSUES (PLI 2006).

Dir. of Office of Thrift Supervision v. Vinson & Elkins, L.L.P., 168 F.R.D. 445 (D.D.C. 1996), *aff'd sub nom*. 124 F.3d 1304 (D.C. Cir. 1997).

District of Columbia Rules of Professional Conduct, Rule 1.3.

Fed. R. Evid. 502(d).

Hewlett-Packard Co. v. Bausch & Lomb, Inc., 115 F.R.D. 308 (N.D. Cal. 1987).

In re Gen. Motors LLC Ignition Switch Litig., 80 F. Supp. 3d 521 (S.D.N.Y. 2015).

In re Kellogg Brown & Root, 756 F.3d 754 (D.C. Cir. 2014).

In re OM Group Sec. Litig., 226 F.R.D. 579 (N.D. Ohio 2005).

In re Pac. Pictures, 679 F.3d 1121 (9th Cir. 2012).

INTERNAL CORPORATE INVESTIGATIONS (Brad D. Brian & Barry F. McNeil eds., American Bar Association 2d ed. 2007).

Kaiser Found. Hosps. v. Superior Court, 66 Cal. App. 4th 1217 (1998).

KAYE SCHOLER, LLP, DESKBOOK ON INTERNAL INVESTIGATIONS, CORPORATE COMPLIANCE AND WHITE COLLAR ISSUES (PLI 2007).

Koumoulis v. Indep. Fin. Mktg. Group, No. 10-CV-0087, 2014 WL 223173 (E.D.N.Y. Jan. 21, 2014).

Largan Precision Co v. Genius Elec. Optical Co., No. 13-cv-02502-JD, 2015 U.S. Dist. LEXIS 2072 (N.D. Cal. Jan. 8, 2015).

Lawson v. FMR, LLC, 134 S. Ct. 1158 (2014).

Mary Patrice Brown & David R. Dorey, Government Announces "Substantial Shift" in Filip Factors for Rewarding Corporate Cooperation with Government Investigations (Sept. 15, 2015), *available at* https://www.omm.com/resources/alerts-and-publications/publications/government-announces-substantial-shift-in-filip-factors-for-rewarding-corporate-cooperation-with-government-investigations/.

Mary Patrice Brown, et al., DOJ Criminal Division Launches One-Year Pilot Program as Part of Enhanced FCPA Enforcement Strategy (Apr. 20, 2016), *available at* https://www.omm.com/resources/alerts-and-publications/alerts/doj-criminal-division-launches-one-year-pilot-program/.

MICHAEL DELIKAT, CORPORATE WHISTLEBLOWING IN THE SARBANES-OXLEY ERA (PLI 2006).

Michael D. Goldhaber, *With Internal Investigations, Firms Walk a Tightrope*, THE AMERICAN LAWYER, May 26, 2016, *available at* http://www.americanlawyer.com/id=1202757857269/With-Internal-Investigations-Firms-Walk-a-Tightrope-?kw=With%20Internal%20Investigations%2C%20Firms%20Walk%20a%20Tightrope&cn=20160526&pt=Am%20Law%20Daily&src=EMC-Email&et=editorial&bu=The%20American%20Lawyer.

NANCY KESTENBAUM, ET AL., INTERNAL INVESTIGATIONS 2009: HOW TO PROTECT YOUR CLIENTS OR COMPANY (PLI 2009).

NLRB v. Weingarten, Inc., 420 U.S. 251 (1975).

Oak Indus. v. Zenith Indus., No. 86 C 4302, 1988 U.S. Dist. LEXIS 7985 (N.D. Ill. July 27, 1988).

Office of Inspector General, OIG Compliance Program Guidance for Pharmaceutical Manufacturers (68 Fed. Reg. 23,731) (May 5, 2003).

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://usdoj.gov/opa/documents/corp-charging-guidelines.pdf.

Report of Investigation, Exchange Act Release No. 44969 [The Seaboard Memo] (Oct. 23, 2001), *available at* http://www.sec.gov/litigation/investreport/34-44969.htm.

Robert W. Tarun, *Tarun's Ten Commandments for Conducting Internal Investigations.* ETHISPHERE, Nov. 2, 2009, available at http://www.bakermckenzie.com/ARCorporateComplianceTarunCommandmentsJul09/.

Ryan v. Gifford, No. 2213-CC, 2007 WL 4259557 (Del. Ch. Nov. 30, 2007).

Sally Q. Yates, Memorandum, Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), *available at* https://www.justice.gov/dag/file/769036/download.

Sally Q. Yates, Remarks at New York University Law School Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (Sept. 10, 2015), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

SEC v. Roberts, 254 F.R.D. 371 (N.D. Cal. 2008).

Securities and Exchange Commission, Division of Enforcement, *Enforcement Manual, Section 6, "Fostering Cooperation"* (Mar. 3, 2010), *available at* http://www.sec.gov/divisions/enforce/enforcementmanual.pdf#6.2.

United States v. BDO Seidman, LLP, 492 F.3d 806 (7th Cir. 2007).

United States v. Fokker Servs. B.V., No. 15-3016, __ F.3d __, 2016 WL 1319266 (D.C. Cir. Apr. 5, 2016).

United States v. ISS Marine Servs., 905 F. Supp. 2d 121 (D.D.C. 2012).

United States v. Kovel, 296 F.2d 918 (2d Cir. 1961).

United States v. Kumar, 617 F.3d 612 (2d Cir. 2010).

United States v. Kumar & Richards, Cr. No. 04-847 (E.D.N.Y. 2004).

United States v. LeCroy, 348 F. Supp. 2d 375 (E.D. Pa. 2004).

United States v. Ruehle, 583 F.3d 600 (9th Cir. 2009).

United States v. Zar, Cr. No. 04-331 (E.D.N.Y. 2004).

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

Wellpoint Health Networks, Inc. v. Superior Court, 59 Cal. App. 4th 110 (1997).

W*ong v. Bd. of Educ. of Cmty. Consol.*, No. 11-CV-07357, 2013 WL 6571326, at *2 (N.D. Ill. Sept. 30, 2013).

Appendices

APPENDIX A: INTERNAL INVESTIGATION CHECKLIST

Opening the Investigation

____ Determine whether a formal investigation is appropriate

____ Define overseeing body

____ Consider need for outside counsel

____ Consider nature of allegations—are there special reporting requirements or privacy obligations requiring immediate attention?

____ Consider need to coordinate with auditors, insurers, or regulators

____ Take steps to ensure that the privilege will be protected going forward

- ____ Set clear protocols governing sharing and retention of information
- ____ Consider joint-defense agreements, if applicable

____ Determine whether there is a known or suspected whistleblower

- ____ If so, consider whistleblower issues

Document Preservation

____ Identify custodians and corporate sources

____ Contact IT Department regarding preservation of new, current, and archived data

____ Place a litigation hold notice

____ Consider engaging a computer forensics expert and e-discovery vendor

Define Scope and Procedures

____ Draft work plan and budget

____ Discuss roles of in-house counsel, outside counsel, experts, and other parties

____ Consider whether initial legal analysis is necessary to guide investigation

____ Schedule regular status updates for the person(s) directing investigation

Document Collection and Review

____ Collect electronic documents

____ Conduct document collection interviews and collect hardcopy documents

____ Process documents

____ Determine if project is appropriate for a provider with automated review capabilities

____ Develop search terms

____ Cull data using search terms and other methods, as appropriate

____ Determine reviewers and review platform

____ Develop review protocol and tagging system

____ Execute review

____ Compile set of key documents

____ Document the processes used to prepare for possibility of later scrutiny by government, courts, etc.

Interviews

____ Create list of interviewees

____ Schedule interviews

____ Decide how to handle counsel for witnesses

____ Decide whether to provide documents in advance to interviewees

____ Create interview outlines and attorney binders

____ Conduct interviews

- ____ Two interviewers
- ____ Upjohn warning
- ____ Close interview with warnings about disclosure and privilege

____ Draft interview memos as soon as possible following the interviews

Drawing Conclusions and Making Recommendations

____ Evaluate the facts

____ Research outstanding legal issues

____ Advise the person(s) directing the investigation of the various options

____ Consider remedial action

- ____ Halt all improper conduct
- ____ Discipline wrongdoers
- ____ Additional controls, remediation, compensation
- ____ Formulate implementation plan for remedial measures

____ Consider notifying the government or other third parties

Closing the Investigation

____ Prepare report

- ____ Consider oral or written
- ____ Determine who receives the report, with privilege issues in mind

____ Make any necessary disclosures

- ____ Consider self-reporting and amnesty programs, if applicable

____ Determine if public relations efforts are appropriate

APPENDIX B: ADVICE TO EMPLOYEES REGARDING GOVERNMENT INTERVIEWS

Being asked to answer questions by law enforcement agents in a criminal investigation can be a stressful and intimidating experience. This is especially true if the agents approach an employee outside the workplace. Employees understanding their rights with respect to being questioned by government agents is very important to protecting the legitimate interests of both the employees and the company. It is not uncommon for employees who answer questions without the advice of an attorney to get themselves into trouble that could have been avoided with sound legal advice.

There are three important general principles regarding employee interviews by law enforcement agents. First, the company may not instruct employees to refuse to answer questions. Such an instruction could be construed as obstruction of justice. Second, employees have a right not to answer questions if they so wish. Third, employees are entitled to obtain the advice of a lawyer before they answer any questions.

If an employee is contacted by a government agent who requests an interview, the employee should be aware of the following[1]:

- The employee has the right to speak to the agent or decline to be interviewed.
- The employee has the right to speak to counsel before deciding whether to be interviewed.
- The agent does not have the right to compel an employee to be interviewed or make statements to the agent; cooperation is entirely voluntary on the part of the employee.
- The agent may suggest that if the employee does not agree to an interview, the employee can be subpoenaed to testify before a grand jury. By agreeing to an interview, however, the employee may not prevent the issuance of a grand jury subpoena.
- If an employee decides to submit to an interview with the agent, the employee can insist on having counsel present.
- If the employee decides to be interviewed, the employee should answer all questions completely, accurately, and truthfully.
- The employee is entitled to terminate an interview whenever he or she wishes and may refuse to answer specific questions.
- If the employee decides not to be interviewed, the employee should politely but firmly state that fact to the agent.
- Finally, employees should be advised that if they are contacted by investigators or prosecutors, they may notify the company's General Counsel before deciding whether to be interviewed. The company should provide telephone or help-line numbers.
- If the employee decides to be interviewed but desires the presence of an attorney, the General Counsel can assist in finding an attorney to represent the employee at the interview. But employees should be advised that the decisions whether to be interviewed, when to have an interview, and who should be present, are the employee's personal decisions, not the decisions of the investigating agency or the company.

[1] *See* "Corporate Compliance," *National Law Journal*, July 25, 1994.

Ask for Identification	1. Should state or federal authorities enter your facility with a search warrant, do the following: a. Ask for their identification. b. Ask for a copy of the warrant authorizing the search, and any accompanying affidavit. c. Give them the designated in-house attorney's number and ask that they wait until lawyers arrive before they conduct the search. They have no obligation to wait, but you should request this in any event.
Call Attorneys	2. Immediately call outside counsel or O'Melveny. Fax or email all papers provided to you by the agents to outside counsel. O'Melveny fax numbers are as follows: Century City: +1 310 246 6779 Los Angeles: +1 213 430 6407 New York: +1 212 326 2061 Los Angeles: +1 949 823 6994 San Francisco: +1 415 984 8701 Washington, D.C.: +1 202 383 5414
Dismiss Non-Essential Employees	3. Dismiss all non-essential employees for the day or, if possible, the length of the search. Obviously, discretion must be exercised here to ensure that the facility continues to operate at an acceptable level.
Do Not Consent	4. DO NOT CONSENT TO THE SEARCH. The authorities may ask you to consent to the search and to sign a form acknowledging your consent. Don't do it. You may jeopardize the ability of your attorneys to challenge the legality of the search at a later time.
Read Warrant	5. READ THE WARRANT. The warrant will describe, often in detail, the areas of the facility that the agents have been authorized to search and the items (documents and the like) that they are authorized to seize. Give them access to those areas in the order in which they wish to see them. If the agents want to inspect an area of the facility not covered by the warrant or seize a document or object not covered by the warrant, you cannot prevent them from doing so, and you should not argue with them about the scope of the warrant. However, state to the agent that in your view the documents or areas are not covered by the warrant, and that you are permitting them to search under protest. If the search exceeds the scope of the warrant, the attorneys for the company may later challenge the legality of the search.

Answer Questions	6. You have no obligation to assist the agents in conducting the search. Should the agents inquire about the location of documents and ask where certain documents are located, answer their questions truthfully, but again, don't sign any "Consent" and don't state that you are "agreeing" to voluntarily provide anything. It is one thing to unlock a file cabinet upon request, but you should not take the agents on a tour of the facility, explain your operations or the documents they have been authorized to seize. It is their obligation to specify the documents sought, and it is your obligation not to obstruct their access to such documents. Simply provide them with the documents or objects they demand.
Privileged Documents	7. SHOULD THE AGENTS WISH TO SEE "PRIVILEGED DOCUMENTS"—DOCUMENTS GOING TO AND FROM ATTORNEYS—TELL THEM THOSE DOCUMENTS ARE PRIVILEGED AND ASK THEM TO WAIT UNTIL YOUR ATTORNEYS ARRIVE TO SPEAK WITH THEM ABOUT THIS ISSUE.
Monitor Search	8. MONITOR THE SEARCH. Make a detailed list of the documents removed and ask to copy the documents before they are removed. You do not have the right to stop the search; however, you have the right to observe the search at all times and make a record of everything the agents do and everything they look at. At least one employee should accompany the agents at all times. As the agents begin reviewing or removing documents, make a record of everything they do and every location searched. If you have access to a video recorder, record the search as best you can without interfering with the agents.
Warn Employees About Interviews	9. All employees should be advised that during the search, questions may be asked of them regarding not only the documents that are seized, but also their and others' duties and responsibilities within the facility. Employees should be advised that the search warrant only authorizes the agents to search for and to seize evidence, not to conduct interviews or speak with employees. The employees are under no obligation to talk to the agents during the execution of the search warrant. Moreover, anything that the employees say to the agents can be used against them, and possibly the company, in later criminal or civil proceedings, even if the agents have not advised the employees of their Miranda rights. All general requests for interviews that the agents make should be referred to, and be handled by, outside legal counsel. You can inform employees that the company will provide them with outside legal counsel if they wish. Do not instruct employees not to speak with law enforcement agents. This could be interpreted as obstruction of justice.

Obtain Inventory of Records Seized	10. At the conclusion of the search, THE AGENTS ARE OBLIGATED TO PROVIDE YOU WITH AN INVENTORY OF ALL ITEMS SEIZED. Such an inventory should immediately be faxed to outside legal counsel. Again, however, you should also take notes yourself during the search, and provide that inventory to outside counsel. Identify any seized records that are necessary to continue operation of your business so that copies can be obtained expeditiously – keeping the list short will increase the speed with which copies can be obtained.
Media Inquiries	11. BE PREPARED FOR POSSIBLE MEDIA COVERAGE. Before speaking with the media, confer first with outside counsel.

KEY CONTACTS

O'Melveny hopes that this handbook has been informative. If you have additional questions on issues arising in the context of internal investigations, please contact any of these lawyers.

Century City

David Kirman	+1 310 246 6825	dkirman@omm.com

Los Angeles

Jim Bowman	+1 213 430 6569	bowman@omm.com
Margaret Carter	+1 213 430 7592	mcarter@omm.com
Jorge deNeve	+1 213 430 6649	jdeneve@omm.com
Steven Olson	+1 213 430 7855	solson@omm.com
Stephen Sullivan	+1 213 430 6221	ssullivan@omm.com

New York

Nicole Argentieri	+1 212 326 2122	nargentieri@omm.com
Ross Galin	+1 212 326 4307	rgalin@omm.com
Andrew Geist	+1 212 326 2207	ageist@omm.com
Mia Gonzalez	+1-212-728-5698	mgonzalez@omm.com
Mark Racanelli	+1 212 326 4403	mracanelli@omm.com

Orange County

David Deaton	+1 949 823 7191	ddeaton@omm.com

San Francisco

Caitlin Bair	+1 415 984 8700	cbair@omm.com
Daniel Bookin	+1 415 984 8786	dbookin@omm.com
Sharon Bunzel	+1 415 984 8939	sbunzel@omm.com
Damali Taylor	+1 415 984 8928	dtaylor@omm.com
Michael Tubach	+1 415 984 8876	mtubach@omm.com

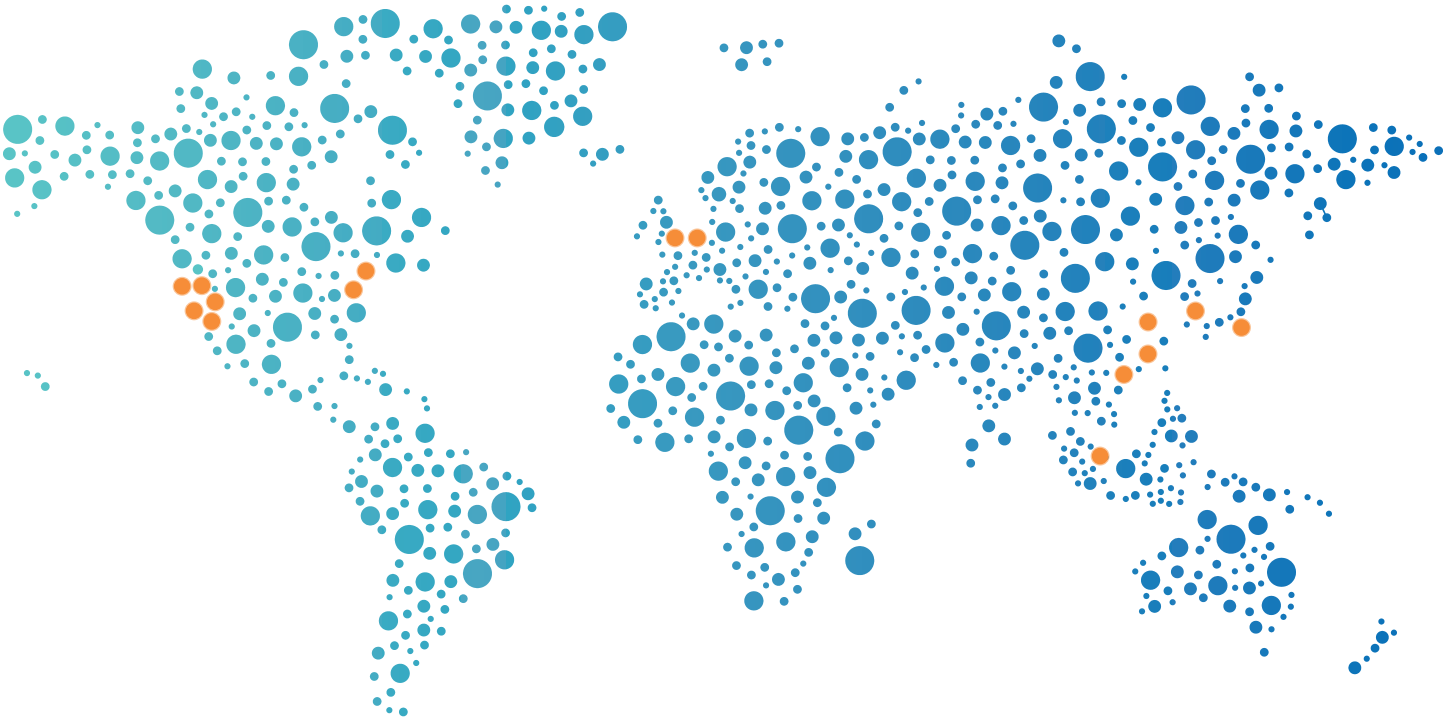
Tokyo

Yoji Maeda	+81 3 5293 2704	ymaeda@omm.com

Washington, D.C.

Lee Blalack	+1 202 383 5374	lblalack@omm.com
Mary Patrice Brown	+1 202 383 5376	mpbrown@omm.com
Howard Heiss	+1 212 326 2116	hheiss@omm.com
David Leviss	+1 202 383 5282	dleviss@omm.com
Greta Lichtenbaum	+1 202 383 5249	glichtenbaum@omm.com
Jeremy Maltby	+1 202 383 5352	jmaltby@omm.com
Lisa Monaco	+1-202-383-5413	lmonaco@omm.com
Benjamin Singer	+1 202 383 5201	bsinger@omm.com

GLOBAL REACH



750 lawyers

15 offices

15 industries

27 practices

Century City • Los Angeles • Newport Beach • New York • San Francisco • Silicon Valley • Washington, DC
Beijing • Brussels • Hong Kong • London • Seoul • Shanghai • Singapore • Tokyo

omm.com