LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication • September 1, 2012

Corporate Internal Investigations

A User Guide for Companies. Part Two of a Three-Part Series

By Vince Farhat, Vito Costanzo and Stacey Wang

Companies are under increasing pressure to investigate and self-report allegations of corporate misconduct. As government agencies become more aggressive in investigating allegations of corporate fraud and abuse, an unprepared company may unwittingly find itself mired in obstruction of justice charges because initial protective steps were not taken to identify and preserve potential sources of evidence and to establish the independence of the company's decision-makers vis-à-vis the alleged misconduct.

This is the second of a three-part series providing companies with a step-by-step guide for planning and conducting sensitive internal investigations into potential wrongdoing. Part One covered the initial decision of whether to conduct an internal investigation and immediate steps that should be taken to preserve evidence and create an independent investigation. Part Two herein addresses how to design and plan internal investigations, including how to define and charter the investigation and document collection and review.

Defining the Scope of the Investigation

Once a company decides to investigate potential wrongdoing, it must define the scope and extent of the internal investigation. This requires companies to balance competing interests. On the one hand, business as usual must go on and companies can ill afford to spend precious resources investigating frivolous and incredible allegations of misconduct. Conversely, credible allegations of misconduct must be investigated and the results documented in a way that will withstand subsequent scrutiny.

One recurring theme is that every case is different; thus, "one size does not fit all" in designing an internal investigation. This investigation may be limited to a handful of interviews and the review of a few documents, or it may be a far-reaching effort involving many witnesses around the country (or abroad) and extensive electronically stored information (ESI). Since there is no set playbook, company investigators must document the process; everything is "on the record" during an investigation. The guiding principle in doing so is how outsiders, such as the government, outside auditors and/or the media, will judge the investigation years from now.

One critical factor in defining the scope of the internal investigation is how quickly the company needs the information. The scope of the investigation can depend, in part, on whether the company wants to complete its investigation before the government becomes aware of the issue, whether the government is willing to defer its own investigation to the completion of the company's internal investigation, the timeline for making any mandated self-disclosures to the government, and the need to establish affirmative defenses for the company. The scope of an internal investigation also can be defined by inquiries from government investigators (whether informal or by subpoena), lawsuits or pre-lawsuit demands, and internal compliance reports from employees or customers.

In line with these considerations, companies should consider the following general factors in assessing the scope of a formal internal investigation.

- How did problem surface and who was involved in reporting the issue?
- How much time does the company have to complete the investigation?
- Is the proposed scope of the internal investigation broad enough to determine whether misconduct occurred?
- Is the proposed scope broad enough to permit the company to take remedial action?
- If the results of the investigation were disclosed, is the proposed scope broad enough to satisfy government investigators?
- What steps must be taken to document the investigation and preserve evidence?
- What will it cost to conduct the internal investigation?
- What steps can be taken to reduce expense without compromising the integrity of the investigation?
- Will the internal investigation disrupt business operations? If so, what steps can be taken to minimize disruption without compromising the investigation?
- Is there a need to maintain confidentiality?

In defining the scope of the internal investigation, the company must identify critical personnel, documents, and internal procedures that could be implicated in the investigation of the potential misconduct.

- What are the elements of the possible civil claims, regulatory viola-

Vince Farhat and **Vito A. Costanzo** are partners and **Stacey H. Wang** is an associate in Holland & Knight's West Coast Litigation Group, resident in the Los Angeles office. They may be reached at Vince.Farhat@hklaw.com, vito.costanzo@hklaw.com and stacey.wang@hklaw.com, respectively.

tions, or criminal charges?
- What employee positions are typically associated with the kinds of events or transactions giving rise to the potential misconduct?
- Who are the employees and/or contractors (regardless of their positions) with potential knowledge of the specific issues under investigation?
- Who are the records custodians for company documents of this type?
- Where are the relevant company records? Don't overlook the possibility that, regardless of company policies, the custodians may have relevant information on their personal computing devices.
- What third parties are typically associated with the kinds of events or transactions giving
- rise to the potential misconduct?
- What customers and/or vendors might have potential knowledge of the specific issues under investigation?
- Where are the above employees, records, third parties located? If any of them are located overseas, consider whether the company needs local counsel and/or local investigators. Foreign laws, such as protections over private information, might be implicated.
- What company procedures are implicated?
- Were company procedures violated? If so, were possible violations documented or recorded?

Chartering the Investigation

After defining the scope of the internal investigation, the company should prepare and formally approve a written document "chartering" the investigation. The Charter can take the form of a resolution from the board of directors or the board audit committee, an engagement letter, or a memorandum issued by senior management or the general counsel. The purpose of the Charter is to:

- Give company investigators the necessary independence and power to conduct an effective investigation.
- Clearly identify the scope of investigation.
- Impose any limitations on the investigators the company deems appropriate.
- Anticipate means to collect and review documents.
- Ensure the company preserves evidence even after the investigation is over, i.e., for use in future related actions such as shareholder derivative suits and other related litigation.

The Charter should be a "living document" because companies may need to re-evaluate the scope of the investigation based on new information and allow the action plan to develop and evolve as documents are reviewed and witnesses are interviewed. Charters for internal investigations should contain a number of the following basic elements.

Specify, where appropriate, that the investigation is being conducted in anticipation of litigation and for the purpose of obtaining legal advice.

Clearly identify the client, i.e., the company, the board of directors, or a board committee.

Describe the scope of the internal investigation.

Identify who is responsible for searching for documents, including Electronically Stored Information (ESI).

Identify who will be interviewed.

Describe how witness interviews will be conducted.

Explain how third party witnesses will be handled.

Describe who the investigators will report to, i.e., entire board, liaison, etc.

Third parties such as customers and vendors often have important information, but contacting them can endanger the confidentiality of the investigation and might jeopardize the company's relationships with these parties. If company investigators decide to interview third party witnesses, the company should proceed very carefully, since missteps can be viewed by the government as witness tampering or obstruction of justice. Therefore, companies should weigh and document the advantages and risks before deciding to interview third parties, such as:

- Maintaining confidentiality versus obtaining information.
- How will the government view failure to contact the third parties versus the potential perception of witness tampering?
- How to establish/maintain credibility with key constituencies?

Directing the Investigation

As part of chartering the investigation, companies must decide who will direct the internal investigation and assemble the investigation team. As discussed in the first part of this article, red flags of wrongdoing sometimes can be quickly resolved by company personnel. For example, a company's human resources department often has the skills and expertise necessary to investigate discrimination or harassment allegations, and a company's audit department often can investigate theft or embezzlement. In these instances, it is strongly advisable to involve in-house counsel to protect attorney-client and work-product privileged information.

Companies may also involve attorneys to direct and plan the internal investigation. It is generally advisable to involve legal counsel where the internal investigation has been triggered by inquiries from government investigators (whether informal or by subpoena), lawsuits, or pre-lawsuit demands. In addition to preserving the attorney-client privilege and attorney work product protection, counsel will bring expertise and experience in conducting investigations and legal advice concerning investigation results.

A related issue is whether the company should rely on in-house counsel or retain outside counsel to conduct the investigation. In some cases, in-house counsel who may have advised management on the issue under investigation could be a percipient witness, or may not be familiar with the investigating government agency. Retaining outside counsel adds to the cost of the internal investigation, but may be justified where the company seeks the perception of greater independence and familiarity with the law enforcement agency. Outside counsel also may be necessary where the company needs additional resources for the investigation.

An internal investigation also may require the assistance of experts such as accountants, engineers, computer forensics, and private investigators. Private investigators should be carefully controlled as they are agents of the company. They should not engage in misrepresentations in order to get information, and the company should not permit investigators to engage in conduct that would be otherwise improper for counsel. The company also should consider using expert retention agreements in conjunction with legal counsel providing legal advice and in anticipation of litigation to as to preserve applicable privileges.

Document / ESI Collection And Review Issues

As a threshold matter, and as discussed in Part One, as soon as a company can reasonably anticipate litigation or a government investigation, all routine actions that would result in the modification or destruction of documents or information, including electronically stored information (ESI), that may be relevant to the litigation or investigation should be suspended. Even if the company does not know particular specifics, the act of enforcing what would ordinarily be a best practice may be viewed as spoliation of relevant evidence or, in a criminal investigation, obstruction of justice. Imaging, or taking a snapshot of, the ESI can provide peace of mind if overriding or modifying data is a concern.

The company should identify and collect an initial relevant universe of hard-copy documents and ESI in the investigative process, not only as part of preserving all evidence, but also to assist in identifying relevant witnesses, framing appropriate topics and questions for interviews, and to refresh witness recollections during

the interviews. In some cases, outside counsel may need to retain technology professionals to forensically retrieve, host, and analyze ESI. In-house IT personnel should only be utilized where the company has a sufficiently sophisticated staff trained in issues that may become critical in a subsequent litigation or in a government investigation, such as chain of custody and metadata preservation.

In a perfect world, all paper documents and ESI would be collected and reviewed before witnesses are interviewed. In the real world, one informs the other; company investigators often start the investigation by gathering documents, but they are not compartmentalized steps. Otherwise, it may be possible to miss clues from witnesses of documents in unexpected places.

Although often tedious, document review can be critical to the goal of learning what happened and why. Investigators should make a written record of what they are doing, including an inventory of what documents have been collected and reviewed, and what search terms have been applied, and organize key documents by topic and by individual. These efforts will minimize the need to re-review possibly voluminous documents.

In the age of electronic storage devices, personal digital assistants, and communications that leave an electronic trail (e.g., texts), potential sources of evidence are everywhere. Understanding the company's technology infrastructure and communicating with the information technology department is crucial. After the initial steps of stopping all automated janitorial and overwriting functions and preserving all relevant back up documents, the company may be facing terabytes (or even petabytes) of data. The unwieldy size of potential ESI is an area that cannot be approached with a "paper" mindset and strategy.

Cloud computing has emerged as a popular way to centralize a company's data. In many ways, cloud computing can make data collection in internal investigations easier. For example, the company's IT personnel can very quickly stop automated functions to preserve data. As well, all networked data for relevant custodians can be collected quickly, sometimes without ever alerting the custodian.

However, even with cloud computing, employees may have relevant communications and data on personal devices. The company must ensure that the employees understand that, depending on the sophistication of the technology, even accessing or viewing a file may look like tampering if the metadata cannot confirm that the file has not be modified. In addition, cloud computing platforms typically involve third-party vendors. Such vendors may be served with government subpoenas without notice to the company. The key takeaway is to be aware that whenever data is maintained by a third party, some control is lost.

Generally, the main concern with ESI is the cost of collection, preservation and review. Where the universe of potential ESI is unwieldy, use of predictive coding and other advanced electronic review tools not only save an enormous amount of money and resources as compared to taking a "banker's box" mentality to document review, it may well be the only means to undertake review of massive amounts of data. Until protocols of general acceptance are developed for computer-assisted collection and review, the trend of the best practice in this area is toward reaching agreement wherever possible. That is, where there is opposing counsel, ideally agreements should be reached, and disputes resolved, before rather than after incurring the expenses for collection and search. The Sedona Principles on the civil side, and the Joint Electronic Technology Working Group's Protocol on the criminal side, have been developed to address best practices in each arena for federal matters, and each continues to be refined. State efforts vary.

As soon as the company realizes that issues regarding ESI will add a layer of complexity, the company should consult outside counsel versed on these best practices, assuming the company does not maintain an in-house ESI group. Not doing so, or going to counsel who insist on approaching the situation with a "paper" mentality, is taking a big risk for expensive missteps down the road.

Conclusion

On a last note, special considerations apply when companies are producing documents in response to government subpoenas, which are not addressed in this guide. The subpoena will often answer many of the questions the company would otherwise grapple with in the absence of the subpoena's directive on the scope of the investigation.

Next month, Part Three of the series will cover witness interviews, memorializing findings, whether to self-report violations, and handling whistleblowers.