

Strategic Considerations When Conducting an Internal Investigation

By Daniel Polatsek, Brian McCarthy, and Scott Woodworth

Workplace fraud is ever present, but in a bleak market, employees increasingly feel the financial pinch in their personal lives. Inhibitions are diminished by stark economic realities, and employees occasionally turn to theft, misappropriation and fraud. The headlines are full of fraudulent schemes both epic and small, from the massive Madoff pyramid scheme to employee theft of materials at the smallest level.

Workplace fraud falls into three general categories. "Asset misappropriation" includes fraudulent invoicing, payroll fraud, theft of trade secrets, confidential information and other intellectual property. "Corruption" is fraud that generally involves acceptance of a bribe, kickbacks through bid-rigging, or use of conflict of interest schemes to obtain an unlawful benefit. For example, where long-time and trusted employees retain favored third-party suppliers in return for kickbacks from those suppliers. Falsification of "financial statements," the third fraud category, consists of material falsehoods in financial statements, such as booking fictitious sales or taking expenses in the wrong period.

To be certain, workplace fraud schemes exist on a far larger and more complex scale than many employers anticipate. These schemes may persist for long periods of time before discovery, and result in huge

Daniel Polatsek is an attorney with Katten Muchin Rosenman LLP. His practice focuses on corporate litigation with an emphasis on internal investigations. Polatsek can be contacted at daniel.polatsek@kattenlaw.com. **Brian McCarthy** is Chief Employment Counsel for Arthur J. Gallagher & Co. and can be reached at Brian_McCarthy@AJG.com. **Scott Woodworth** is an Account Manager with ACT Litigation Services and can be reached at swoodworth@actlit.com

losses. According to the 2008 ACFE Report to the Nation on Occupational Fraud and Abuse, the average fraudulent scheme costs an organization \$500,000 in cases where two or more employees colluded, not including the cost of any litigation, remediation, and lost productivity.

Whether a fraud comes to light through the company's internal or external audits and controls, an anonymous tip from within, from law enforcement, or by accident, a company's first step should be to conduct an internal investigation. The company must determine the nature and extent of wrongdoing, who is affected, and who is to blame. A well-planned and carefully executed investigation can help the company defend itself from potential civil and sometimes criminal liability. In addition, an internal investigation helps a company cast itself as proactive and minimize any negative perception that can accompany the discovery of unlawful conduct (*i.e.*, management is out of touch with what is occurring within their own business).

The linchpin to a successful and productive internal investigation rests on planning. This article discusses a few of the broader strategic considerations in-house or outside counsel should consider prior to committing to any particular course of action.

WHERE TO BEGIN

Generally, engaging outside counsel to organize and conduct an internal investigation is desirable because the company may engage an experienced and objective resource whose communications are largely protected by the attorney-client privilege. To ensure that the protections of the attorney-client privilege are maximized, it should be made clear that: 1) outside counsel is being retained for the specific purpose of rendering legal advice in connection with the investigation of potential unlawful conduct; and 2) within the course of this engagement,

outside counsel will be developing facts and assessing potential legal exposure in anticipation of civil or criminal litigation.

'QUIET' v. 'NOISY'

An important factor to consider up-front is how "noisy" an investigation should be. In other words, will the investigation be transparent and public as it is occurring, or will the decision be made to keep it confidential and known only among the few individuals actually conducting the investigation. A variety of factors will dictate a company's decision. For example, if the suspected wrongdoing is already generally known (*e.g.*, news media or industry/employee blogs) the best decision may be to openly acknowledge the investigation with a statement that the company is taking the suspected wrongdoing seriously. A "noisy" investigation of this type can also give the company control over the timing, manner and content of disclosures about the underlying wrongdoing. In this way, a company can have a hand in managing public perception and present itself as being proactive, as opposed to appearing caught off guard, out of touch and reactive.

Consider, however, that if suspected unlawful conduct has not already become public, the "noisy" avenue may create risks to the preservation of important evidence. Specifically, a "noisy" approach may permit individuals on the periphery of a fraudulent scheme to destroy or remove important physical and electronic evidence. It is often impossible to know at the beginning of an investigation the breadth and scope of a fraudulent scheme. As a result, the public acknowledgement of an internal investigation may allow the targets of the investigation (as well as their co-conspirators operating on the periphery of the scheme) to destroy or remove important physical and electronic evidence. A company must weigh the risk of public disclosure against tipping off conspirators to the fraud.

CHOOSING THE PLAYERS

After outside counsel is retained, the question then becomes, "who will assist counsel?" Because a well-orchestrated fraudulent scheme is generally not fully understood at the outset of an investigation, the individuals assisting counsel should be limited to a select few such as a chief financial officer, chief operating officer, internal auditor, or an executive-level IT professional.

Often, a chief financial officer, chief operating officer, or internal auditor has institutional knowledge of operations and record-keeping that may include where relevant hard-copy files are located (e.g., expense reports, invoices, time sheets and personnel records). Those same individuals may have invaluable insight into a company's culture that will assist in an effective investigation. An executive-level IT professional can assist counsel in identifying and preserving electronic evidence that might otherwise be inadvertently deleted (through a standard document destruction policy), or intentionally destroyed by those under investigation.

By identifying and employing a select team of individuals to assist counsel, the chances that the investigation will be compromised before it has a true opportunity to begin is significantly reduced. This approach minimizes the risk that important evidence will be destroyed by those directly under investigation or their co-conspirators, while maximizing the protections of the attorney-client privilege.

LAUNCHING AN INVESTIGATION

Obviously, the primary goal of an internal investigation is getting to the bottom of suspected unlawful conduct and putting a stop to it. Understanding the full extent of the wrongdoing requires an understanding of the who, what, when, where and how of the scheme.

Organization is key. Prior to initiating an investigation, counsel should prepare an outline detailing exactly how the investigation will proceed, including a schedule of tasks, deadlines and how evidence will be memorialized and preserved. Effort should be made up-front to decide which employees to interview and how the interviews will be conducted. For example, it may be advantageous to simultaneously interview employees suspected of wrongdoing to prevent them from coordinating explanations for suspicious conduct.

It is almost always a good idea to have a third-party witness or investigator present for key interviews to avoid potential disputes as to what was said and to whom during the interview. The presence of a third party can also help corroborate that at the outset of the interview, it was explained by counsel that they represent the company and do not represent the individual (and thus, the interview is not protected by the attorney-client privilege).

Regardless of the type of wrongdoing, it is rarely a good idea to create a fact witness of an executive whose sworn testimony could potentially bind the company in subsequent legal proceedings. Therefore, the urge to include company executives in the interview process should be resisted.

WORKING WITH THE DATA

It is also important to understand what data means to an investigation and the strategic considerations it entails. A good start is to identify the potential custodians of data and understand where all of their data is located. For example: 1) is it on desktop hard drives, laptop hard drives, share drives, e-mail exchange server, backup tapes or voicemail, to name a few possible sources? 2) did the relevant custodians use their home computers? and 3) can the collection process take place during normal business hours or must it occur after hours?

A great resource at the outset of any larger internal investigation is to contact an IT executive and see if the company has a data map of where each custodian's data resides. This makes identifying the data population much easier and provides much needed direction to an outside supplier retained for the purpose of collecting electronic data.

Once the data population has been identified, the next step, if it was not documented previously, is to design a cost effective process workflow. As evidenced by the recent corrupt payment investigation at Siemens, this process has the potential to be very expensive. According to its public statement at the conclusion of Siemens's investigation, investigators electronically searched approximately 82 million documents and then reviewed approximately 14 million documents in connection with their determination of whether Siemens had complied with certain anti-corruption regulations.

Generally speaking, it is a good idea to proceed with the data-collection process as if the company was in the midst of planning

to make a formal document production to the government or to another civil litigant. By engaging in a formal data collection process and memorializing those efforts, the company is able to effectively demonstrate the tangible results of its investigation and how and why it may have reached certain conclusions. In addition, this formal collection process allows in-house or outside counsel to identify documents protected by the attorney-client privilege.

It is important to note that while potentially costly, there are options in reducing the cost of a formal data collection while culling the data population effectively. For example, one option is for counsel to find a supplier capable of allowing a company's legal team to cull documents electronically at the folder level or by file type. This can result in a significant reduction of the population and therefore, reduce costs by narrowing the pool of relevant documents and the number of documents in the review process. Once the culled population has been identified, it can be processed using additional strategies such as keyword and date filters, de-duplication and concept search options.

CONCLUSION

A company faced with the discovery of fraud within its ranks faces a number of critical decisions and should consider each of them with the guidance of experienced in-house or outside counsel. Time is often of the essence, and particularly so in the case of evidence preservation, disclosure strategy and cooperation with law enforcement agencies. A well-planned and carefully executed investigation may or may not be able to mitigate the losses a company has already suffered, but it will go a very long way in mitigating possible civil and criminal liability for the company, as well as negative public perception that inevitably follows the discovery of internal unlawful conduct.