

PUBLICATION

Data Driven Part One: How to Use Data to Achieve an "Effective" Internal Investigation [Ober|Kaler]

August 01, 2014

With the increase in government scrutiny and enforcement actions against corporations for fraud, internal investigations are becoming the norm throughout corporate America. Whether initiated on the heels of an employee tip about internal misconduct, or in response to a government-issued subpoena that suggests possible violations of criminal law, conducting an internal investigation remains one of the most effective ways for a corporation to ascertain whether a credible allegation of wrongdoing exists.

What is an "effective" internal investigation? Specific company definitions may differ greatly from one another. Fundamentally, an effective internal investigation enables a company to determine whether wrongdoing did, in fact, occur and to assess the potential legal risks and exposure that may flow from that misconduct. A company's ability to assess those risks depends on the quality of the information gathered during the investigation and how that information is analyzed.

This is the first article in a two-part series providing companies with practical advice on the role of data in an internal investigation into potential wrongdoing. This article outlines two hypotheticals and then suggests types of data to gather during an internal investigation.

Gather All Relevant Data

First, companies must gather all relevant data early in the process when they undertake an internal investigation. In general, that data will come in the form of electronic data, hard-copy documents and witness statements from interviews the company will need to conduct; however, each company's profile or makeup is different. To determine the most relevant data, outline all issues under investigation and the people (custodians) likely to possess information. Companies should consider memorializing thoughts and strategic approaches in an investigations plan, which will serve as a "road map" as the investigation unfolds.

Documents: Beginning Considerations

To illustrate the types of data that companies should consider obtaining and analyzing, we offer two hypothetical examples. Our first hypothetical involves an American-owned, publicly traded company that uses a foreign-based distributor to sell its products. This company initiates an internal investigation because it receives information that a foreign-based distributor allegedly pays bribes to foreign government officials to sell the company's products, in violation of the Foreign Corrupt Practices Act (FCPA).¹ In this scenario, the data the company should request may come in different forms. Let us assume that the company has first conducted the initial inquiries to determine that the tip has some credibility and requires further investigation. During its investigation, the company then should examine:

- the distributor agreement;
- due diligence files; and
- identified accounting records, specifically: the cash disbursements ledger, the detailed vendor master file and the chart of accounts.

The second hypothetical involves an American company that is the largest seller of hearing aids in the U.S. The sales team markets its products to Ear, Nose and Throat (ENT) physicians, many of whom have patients whose insurance is Medicaid, which will pay for medically necessary hearing aids. Assume, in addition, that there is a complaint on the company's hotline that a few members of its sales team are encouraging the ENT physicians to prescribe medically unnecessary hearing aids as a way of increasing sales. To investigate this allegation—which might have False Claims Act and Federal Anti-Kickback Statute² implications for the company—the company would want to gather data related to marketing, a list of the physicians targeted and accounting/financial records (including the marketing budgets, sales persons' individual budgets and sales force compensation records).

Next, regardless of the subject matter of the investigation, it is advisable that companies gather all potentially relevant documents maintained in paper or electronic format. Depending on the records custodians and how they keep documents, data may be found in spreadsheets, memoranda, e-mails, electronic calendar entries and voicemail messages. It may also be found on company-issued smartphones (e.g., in text messages).

How companies access the data that they need to thoroughly investigate the issues depends on a variety of factors. For example, if companies conduct an internal investigation and have not received a government subpoena, but want the investigation to remain confidential, they should consider enlisting other component parts of their organizations (e.g., the IT department) to remotely obtain documents and provide access to e-mail accounts and the individual share drives of each custodian or department.

If, however, companies have received a subpoena, they will need to issue a document preservation notice.³ Depending on the circumstances, companies also may need to enlist a computer forensic expert to retrieve and preserve data relevant to its investigation.

Documents: Investigative Due Diligence on Subject(s)

It also might help to take time to better understand the people who allegedly engaged in the purported misconduct (i.e., the "subjects" of the investigation).⁴ This could provide additional information into the mindset of the subjects when they engaged in the conduct or could inform the company regarding the circumstances surrounding the alleged wrongful activity.

For example, with respect to the hypothetical allegations against the foreign distributor making bribes, a search of civil court filings may indicate the company has recently entered into bankruptcy proceedings or been involved in protracted civil litigation, which may have provided the distributor the need to increase cash flow through product sales. Additionally, on-the-ground investigative steps may uncover that the distributor has hired a former government official's relative to work in the company. A few key steps from there include:

- conducting database searches of news media, including both English and foreign-language search criteria; both public and private databases, including asset holdings of third parties; and social media activity, including Facebook, LinkedIn and Twitter; and
- conducting private-source inquiries with industry and local confidential sources, one of the best forms of gaining background because in many cases, individuals and companies are located in close-knit communities that are hard to penetrate and for which it is hard to gain useful information from common interviewing techniques.

In both hypothetical scenarios, companies should consider gathering personnel records. Performance evaluations and disciplinary action information may be instructive. So, too, are compliance-related records. Were there prior complaints of a similar nature? What kind of anti-bribery, False Claims Act or anti-kickback

training did the staff receive? For the hearing aid company, records that outline the compensation structure for the sales force, including salary and bonus information, could prove helpful. The financial records that relate to the sales force's marketing budgets could be, too. Is the company offering incentives to physicians to prescribe medically unnecessary hearing aids?

Assembling information on the subject(s) of the internal investigation will help identify potential key relationships and connections. It could also aid in understanding the subjects' possible financial motives for having engaged in the alleged wrongdoing.

Witnesses

A crucial source of data for fully understanding how potential misconduct occurred is to interview the individuals with knowledge of the facts under investigation. Companies should consider conducting at least two types of interviews. The first type, witness interviews, is designed to provide a full understanding of the alleged activity. In general, a witness is someone who can provide information relevant to the investigation, but who has no potential legal exposure because of the alleged activity. In our two hypotheticals, the companies' witness list may include company personnel from the marketing, accounting and sales departments, including supervisors or other upper management members.

In addition, for the interviews to be protected by the attorney-client privilege, all interviews should be conducted by legal counsel or individuals working at the direction of legal counsel, and should be conducted for the primary purpose of obtaining legal, rather than business, advice.⁵

It is important to remember that different witnesses may have different pieces of information that could be of use, so companies should not think too narrowly about who may, in fact, have important information.

In the medical device kickback scenario—assuming that the investigation has revealed that only a few rogue employees may have provided kickbacks to doctors, unbeknownst to management—it might be appropriate to interview the business development manager who supervises the subject(s) of the investigation. Interviewing the manager could help understand the company's marketing strategy and the kinds of appropriate marketing expenditures for its sales force. After obtaining the subjects' lists of physician clients, the company might have some follow-up questions for the manager. In addition, after obtaining financial records related to the subjects' marketing and entertainment expenses, it might be appropriate to speak with that business manager or people in the accounting department to determine how the subject employees were able to conceal their wrongdoing (i.e., did the subjects falsify documents)?

As for the distributor hypothetical, it might be important to interview individuals who work for the distributor to determine how it sells products to customers, including government entities, and how those processes compare to the manner in which the distributor actually sells the company's products. Through its review of the distributor agreements, the company should have a good idea of who needs to be interviewed, such as the primary contact with the company, sales people that handle its accounts and—to the extent available—the distributor's management. In addition, a review of the accounting and electronic records will provide ample information to ask the right questions and determine if the answers provided make sense. The statements that the company obtains from the distributor's employees may prove crucial to determine, for example, whether the distributor has bribed government officials or whether one of the company's employees is involved in the alleged misconduct.

In addition to conducting witness interviews, companies should consider whether it is possible to interview the subject of the investigation. If they decide to interview the subject, it is advisable to conduct a subject interview

after gathering enough information to determine if the allegations of wrongdoing are credible. The timing of the subject interview is extremely important, because they might only have one opportunity to speak to the subject. Once employees become aware that an investigation has begun, people involved in the wrongdoing may become uncooperative, retain legal counsel or leave the company.⁶ In addition, subject interviews should always be done with more than one person present. Preferably, one person should take notes while the other person asks questions. This helps to avoid a possible "he said/she said" claim by the subject. Because investigations can last for several months and even years, these interviews should be well documented and memorialized in written interview memoranda.

Exculpatory Findings

Finally, if companies find themselves under government investigation, they must ask some questions, such as: did it gather all exculpatory evidence? Did it look for and obtain evidence that tends to suggest that the company acted honorably or that the conduct was limited to a rogue employee? Or did it find evidence that although a few missteps—or lapses in judgment—occurred, there was no civil or criminal wrongdoing? As we will explain in greater detail in Part Two of this series, appearing in the Aug. 8 CORPORATE LAW & ACCOUNTABILITY REPORT, exculpatory evidence could aid companies if they are under government investigation and trying to resolve the matter favorably.

Conclusion

As a company's internal investigation unfolds, the data that it gathers will come in many forms, from documents and interviews to media reports to on-the-ground confidential investigative techniques. Getting the right data in an efficient time frame is of paramount importance to conducting an effective investigation.

Part Two of this series, appearing in the Aug. 8 CORPORATE LAW & ACCOUNTABILITY REPORT, will suggest how to analyze the information that companies have gathered in order to better evaluate whether misconduct occurred. We will also outline some of the issues surrounding the company's use and disclosure of that data.

¹ 15 U.S.C. §§ 78dd–1 et seq.

² 31 U.S.C. § 3729 et seq., and 42 U.S.C. § 1320a– 7b(b)(2)(B).

³ A document preservation notice is a written notice that an organization gives to employees that they must preserve and not alter or destroy records that the government has requested.

⁴ The terms "target" and "subject" are normally used in grand jury proceedings to identify the potential culpability of an individual or company. U.S. Attorney's Manual § 9-11.150. However, for our hypotheticals, we will refer to an individual who may have committed the alleged wrongdoing as a "subject."

⁵ See, e.g., *In re Cnty. of Erie*, 473 F.3d 413, 417 (2d Cir. 2007); *United States ex rel. Baklid-Kunz v. Halifax Hosp. Med. Ctr.*, Case No. 6:09-cv-1002 (M.D. Fla. Nov. 6, 2012); *United States ex rel. Barko v. Halliburton Co. et al.*, Case No. 1:05-CV- 1276 (D.D.C. Mar. 6, 2014).

⁶ Though some companies require employees to cooperate in internal investigations or face disciplinary action, many companies do not have not such a policy.

Reproduced with permission from Corporate Accountability Report, 12 CARE 31, 08/01/2014. Copyright 2014 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>