PUBLICATION

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

August 11, 2014

This is the second of a two-part series providing companies with practical advice on the role of data in an internal investigation into potential wrongdoing. Part One set forth two hypotheticals and discussed information to gather during an internal investigation (12 CARE 898, 8/1/14). This second installment covers how to analyze the data obtained during the investigation, as well as issues related to the disclosure of investigative findings.

Analyze Relevant Data

Part One outlined two hypotheticals: one involved an American-owned company that uses a foreign-based distributor and a potential Foreign Corrupt Practices Act[1]violation; the other involved an American-based durable medical equipment supplier and possible violations of the False Claims Act or Anti-Kickback Statute.[2]

In the first hypothetical, the company faces a potential FCPA violation; namely, a distributor in a foreign country is allegedly paying bribes to foreign government officials to sell the company's products. In Part One, we discussed relevant data to assemble. Here are suggestions on how to analyze that relevant data:

- *Regarding the distributor agreement*: The distributor agreement will hold many keys to the type of additional data the company may want to review. It will assist in determining the means by which the distributor is paid, either through commissions of sales ("commission-based agreement") or a discount from products' list prices ("discount-based agreement"). It will also provide insight on the customer base of the distributor: some distributors sell mainly to private entities, while others may focus on government buyers. If government buyers are involved, then governmental requests for proposals often will be available to review. The distributor agreement will also provide important information regarding who within the organization is responsible for this distributor, what interactions and correspondences exist with the distributor, and which distributor employees may be involved in the conduct. This information will also assist in gathering data by determining who should be on the interview and custodian list.
- *Regarding the due diligence files*: If the company conducts due diligence or provides onboarding procedures for its distributors and maintains due diligence files, it is imperative to review and analyze these documents. This analysis will provide the investigative team with insight into the life of the distributor and its dealings with the company. It will be important to note in the company's review if there have been major changes with the distributor over time (e.g., change of ownership, change in location) and whether the company has conducted additional due diligence steps (or updated steps) throughout the life of the distributor.
- *Regarding the accounting records*: As the investigation focuses on a specific event for a specific entity, there is no need to request the company's entire detailed general ledger. However, it is important to obtain and review all transactional accounting records for this particular distributor. These records will consist of accounts payable voucher packages including invoices, purchase orders, payment requests for commissioned-based distributors, or sales and shipping records for a discount-based distributor. No matter which type of distributor the company deals with, it is important

to get enough data to conduct the analysis both in time frame and volume of transactions. The time frame associated with the scope of the investigation is important, and the company must consider how far back in time its review will go. One consideration is to go far enough back to make an intelligent comparison between the distributor's present and past activities, to see whether it has any changes or inconsistencies in its relationship with the company. Normally, at least two years of activity prior to the alleged incident should be reviewed. Next, it is important to review enough transactions to identify trends in the data that may point to illicit behavior. If your sample of transactions is too small, the company may not be able to uncover and properly investigate the allegations.

In the second hypothetical, the company is the largest hearing aid seller in the U.S. and there are allegations that a few rogue employees may have provided kickbacks to certain physicians in order to increase sales. These kickbacks induced the physicians to prescribe medically unnecessary hearing aids. In Part One, we identified relevant data. Here are some suggestions on how to analyze that data:

- *Regarding the marketing materials*: Gather memoranda, e-mails, outlines, and/or directives and policies written by supervisors regarding how to market the hearing aids to physicians. The company should also gather the marketing and development plans for the specific employees under investigation. The goal is to understand what sales presentations should have been given to physicians and whether those presentations are consistent with the law. The company needs to understand its possible legal exposure if the government learns of this alleged misconduct—namely, will the government be able to establish that the company encouraged the alleged wrongdoing for financial reasons that are at odds with the law? Consider two questions while reviewing these materials: What were the sales goals for the employees under investigation? What incentives existed for the employees to meet those goals?
- *Regarding the personnel records*: Gather personnel records, especially salary and bonus information for the alleged rogue employees. While reviewing records, ask how much compensation, both in the form of a salary and a bonus, the subject employees received before and during the years under investigation. It might be a fact of significance if the employees did not receive bonuses because their sales were low before the years under investigation, but they received large bonuses during the years under investigation. The company might need to interview the employees' supervisors to ascertain whether and how they incentivized employees to increase sales. The aim is to understand whether incentives existed for the salespeople, and whether those incentives may have inadvertently encouraged certain behaviors that the government, if it decides to investigate, might find questionable. The government will look for financial rewards as evidence of motive for committing wrongdoing.
- *Regarding the compliance training materials*: Companies should obtain these materials and ask the following questions as a starting point: Were antikickback and false claims training offered to the subject employees? If so, how many hours of training were given? How frequently was the training offered? How in-depth was the training? How often did the employees attend the training?

  The sales employees might not have received adequate training on how not to violate the law, or they may have received ample training, but ignored it. If the company faces a government investigation, the government will be interested in evidence of its compliance culture.
- *Regarding the information on subject employees' clients*: Who are the specific doctors to whom the employees sold hearing aids? Do these physicians have patients who participate in Medicaid? Review the data to determine whether there are patterns: did certain doctors always prescribe two hearing aids, rather than one, for all patients? Or is there something about the timing of the prescriptions that suggests these physicians were given cash or other rewards based on the number of prescriptions they wrote?
- *Regarding the marketing budget and expense reimbursement records for the subject employees*: Analyze this information to determine whether illegal payments occurred. For instance, were

physicians paid to speak at nursing homes with the intent to increase the number of prescriptions that they might write? Were physicians paid in cash; given tickets to sporting events; or rewarded with expensive trips, meals and/or gifts in return for agreeing to write medically unnecessary prescriptions?

Disclosing the Data: Special Considerations- Board of Directors and Outside Auditors

At the conclusion of the investigation, the company will have many issues to consider, including what type of report to provide to its board of directors. At first glance, it would seem appropriate that a comprehensive written report should be prepared that outlines the investigative protocols used, findings and the suggested remediation efforts. However, a written report may not always be what the board requires. The board may prefer an oral presentation of the investigative steps, accompanied by a summary PowerPoint that outlines the key findings of the investigation. The presentation should also include any additional follow-up investigation that may be required.

Another disclosure that the company might have to make while the internal investigation is pending relates to requests from its outside auditor. An outside auditor is required to audit litigation reserves and assess the potential impact that the result of the investigation may have on the company, and determine how to document the same in company financial statements. If the auditor concludes that the investigation may have a material effect on the company's finances, certain loss contingencies must be disclosed to the public. Once an auditor is made aware of the investigation, it will likely have many questions. It is important to determine specifically what the auditor is looking for and to focus your responses to answer its questions. Consult with legal counsel to determine if any documents, including legal opinions, attorney-client privileged materials or workproduct materials, should be provided to the auditor. Be careful not to waive any legal privileges, while at the same time providing the auditor with all available information regarding the investigation.

Disclosing the Data and Cooperation With Regulators

A question that arises with all internal investigations is if and when to self-report the investigative findings to the government and, if the company is under government investigation, to what extent the company should cooperate with the government in the hope of receiving leniency. A company may consider several options. For instance, after evaluating a variety of factors and obtaining appropriate legal and accounting advice, a company may decide to publicly disclose the investigation in its Securities and Exchange Commission filings, but not to otherwise provide further information to investigators unless required to do so.

In deciding whether to self-report to the government, a publicly traded company should evaluate whether it is required to disclose the investigation based on federal securities laws. Though there is no statute that explicitly states that an investigation must be self-reported to investigators, certain SEC regulations require public disclosure when an investigation has determined that a government entity may file a legal proceeding against the company or an officer, or when a director is a defendant in a legal proceeding. Companies routinely make such disclosures in their SEC Form 8-K filings, and lack of proper disclosure may expose a company to additional fines and penalties. Once public disclosures are made, the self-reporting decision is practically made for the company.

However, companies should recognize that the U.S. Department of Justice and SEC have made it publicly known that they reward self-reporting and cooperation in cases involving FCPA violations. Specifically, they have said they both "place a high premium on selfreporting, along with cooperation and remedial efforts, in determining the appropriate resolution of FCPA matters."[3]

In DOJ cases, prosecutors evaluate a company's cooperation pursuant to the PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS.[4] Additional guidance about how the government weighs a company's cooperation can be found in the U.S. Sentencing Guidelines.[5]

Practical examples exist of how the DOJ and SEC evaluate self-disclosure and cooperation. For instance, in a recent FCPA case against Marubeni Corp., which pled guilty and agreed to pay an $88 million fine, in reaching a resolution, the DOJ considered factors such as "Marubeni's decision not to cooperate with the department's investigation when given the opportunity to do so, its lack of an effective compliance and ethics program at the time of the offense, its failure to properly remediate and the lack of its voluntary disclosure of the conduct."[6]

There is one final consideration related to the decision to self-report investigative findings to the government. If the investigation was conducted with the assistance, and at the direction, of legal counsel, work would generally be protected by the attorney-client and workproduct privileges. In making a self-reporting decision, the company needs to evaluate several factors to decide whether waiver is appropriate.[7]For instance, if the company is under government investigation and wants to demonstrate its good faith to the government, it may decide to share both the unfavorable and favorable information that it unearthed during the investigation.

For instance, through witness interviews and document review, the company may have discovered that its top hearing aid salesperson was a rogue employee who deliberately violated the company policy against kickbacks. The company might also have discovered that while he was responsible for $1 million worth of sales in a year, his supervisor immediately suspended and then fired the employee when he learned of the conduct. Thus, the company has a scenario where it could be beneficial to share with the government what it has learned to try to persuade it that the company should not face FCA or other liability. The full disclosure of investigative steps, thought processes and actions may require the company to waive privileged information. And once the privilege is waived, the information may be accessible to third parties for use in adverse actions against the company (e.g., in the form of derivative actions or other civil litigation against the company or the board of directors). Thus, the company should carefully weigh the risks and benefits of such disclosures and seek appropriate legal advice.

Conclusion

An "effective" investigation requires gathering and analyzing data from a variety of sources. Key factors to weigh include how the company plans and executes its investigation; how it gathers electronic and paper data; the people the company chooses to interview; and how, when and to whom the company discloses information. Whether the company's distributor in a foreign country is bribing government officials or the company has a rogue employee paying kickbacks to physicians, conducting an internal investigation is still the most effective way to determine whether a credible allegation of wrongdoing exists and whether wrongdoing occurred. An internal investigation enables a company to assess its potential legal risks and the possible exposure that may flow from that misconduct.

[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] CRIMINAL DIVISION OF THE U.S. DEP'TOF JUSTICE AND ENFORCEMENT DIVISION OF THE U.S. SEC. &EXCH. COMM'N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT 54 (Nov. 14, 2012), available at http://www.justice.gov/criminal/fraud/fcpa/ guide.pdf
[4] PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS § 9-28.700 (2008).
[5] U.S.S.G § 8C2.5(g) (2013).
[6] U.S. Dep't of Justice, Marubeni Corporation Agrees to Plead Guilty to Foreign Bribery Charges and to Pay an $88 Million Fine (Mar. 19, 2014), http://www.justice.gov/opa/pr/ 2014/March/14-crm-290.html

[7] It should be noted that cooperation credit no longer depends on the waiver of attorney-client privilege information, but must focus on the willingness and sufficiency of a company's disclosure of facts that would aid in the government investigation. See PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS §§ 9-28.710, 9-28.720.