Preparing for an FCPA Investigation Before You Are Under Investigation


Imagine that you are the chief compliance officer of a multinational corporation headquartered in the United States. One day, without warning, you receive a broadly worded subpoena from the U.S. Department of Justice (DOJ) seeking information about your business activities in Africa, Eastern Europe, Latin America, and the Middle East. You contact the prosecutor who issued the subpoena and learn that the DOJ has launched a Foreign Corrupt Practices Act (FCPA) investigation after receiving a tip that your company’s subsidiary in North Africa authorized a third-party consultant to bribe government officials to obtain sales contracts. The government wants to know all about this alleged incident, your compliance program, and whether similar incidents might have occurred in the other high-threat, high-risk markets where you do business.

For many in-house legal and compliance personnel, this is a nightmare scenario that marks the beginning of a lengthy, expensive, and carefully choreographed government investigation. Even if the DOJ does not ultimately conduct an enforcement action, the investigation could stretch for years, as prosecutors seek to overturn every stone in search of corrupt behavior, resulting in significant legal fees, management distraction, and harm to your company’s reputation. Unfortunately, this scenario is all too familiar in the current enforcement environment, even for responsible companies that have taken steps to address corruption-related risks.

As U.S. regulators dramatically accelerated their efforts to enforce the FCPA over the past ten years, white collar criminal defense lawyers and compliance professionals spilled much ink over the need for multinational companies to implement effective ethics and anti-corruption compliance programs to prevent violations. Many companies that do business outside the United States took this guidance to heart and spent vast sums of money developing extensive anti-corruption policies and procedures.

While robust anti-corruption compliance programs surely help prevent many FCPA violations, recent enforcement activity demonstrates that even those companies with relatively substantive compliance programs are vulnerable to extensive government investigations and prosecution for the acts of their employees. For example, in November 2010, Noble Corporation settled civil and criminal FCPA charges that were brought by U.S. regulators despite the fact that the company

---

* Suzanne Rich Folsom is Senior Vice President, Chief Regulatory & Compliance Officer and Deputy General Counsel at ACADEMI LLC, a leading training and innovative security solutions company headquartered in Arlington, Virginia. Victoria McKenney is Director, Regulatory & Compliance and Associate General Counsel at ACADEMI LLC. Patrick F. Speice, Jr., is Compliance Counsel at ACADEMI LLC.
had a pre-existing anti-corruption compliance program and that the allegedly improper payments were authorized by several employees in violation of applicable policies and procedures. Similarly, Morgan Stanley was under FCPA investigation for more than three years due to the misconduct of a senior executive before the DOJ finally concluded in April 2012 that the company’s robust compliance program meant that it would not be charged for the misconduct of one employee. These examples show that no compliance program can prevent the possibility of employee misconduct and that companies should therefore assume that they may come under scrutiny at some point and prepare accordingly. Armed with the knowledge that a robust compliance program is the best insurance against government prosecution, companies need to ask what steps they can take to mitigate the negative impacts of an investigation before it even begins.

**Appropriate Preventive Controls and Documentation**

At the center of any effective anti-corruption compliance program is a set of written policies, procedures, and other internal controls that are designed to prevent improper payments from being made on behalf of the company. These controls might include, among others, a code of business ethics and conduct, an anti-corruption compliance policy targeting the FCPA and other applicable anti-corruption laws, employee screening procedures, pre-retention business partner due diligence requirements, limitations on provision of business courtesies, and training to educate employees about applicable laws and regulations. The DOJ has required numerous companies that have settled FCPA claims in recent years to agree to implement such controls as a condition of settlement, and the U.S. Sentencing Guidelines applicable to corporations recognize that these controls are an important component of an effective ethics and compliance program. In addition, various international, non-governmental, and non-profit organizations that work to combat corruption, including the Organisation for Economic Co-operation and Development, Transparency International, and the World Economic Forum, recommend that companies implement these types of controls to prevent bribery and help ensure compliance with applicable anti-corruption laws.

A company that has strong preventive controls in place can often demonstrate to regulators that it is committed to ethical business practices and that any misconduct is the result of circumvention by a rogue employee and not a culture of corruption or a systemic weakness. Accordingly, it may be able to persuade regulators that the investigation need not expand beyond the operations implicated in the allegations to other operating units or geographic locations.

Simply having controls in place may not be enough, however, and a skeptical regulator that has learned of alleged misconduct will likely want to confirm that the company’s controls are both appropriately designed and operating effectively before concluding that the misconduct is an anomaly. To that end, it is essential that a company document its compliance efforts. For example, training records showing that an implicated employee received regular anti-corruption training or due diligence materials demonstrating that the company thoroughly vetted the
allegedly corrupt third party at issue can serve as proof that misconduct occurred despite the company’s best efforts to guard against it. In addition, a company should continually review and adjust its controls to ensure that they are appropriately designed and working as intended. Such monitoring can be conducted through periodic risk assessments, formal audits, and less formal verification and testing activities. Again, documenting the results of these activities and any resultant remedial measures is important to evidence the company’s efforts to maintain a best practices compliance program.

**Policies and Procedures for Detecting and Reacting to Misconduct**

In addition to preventive controls, any effective compliance program must have policies and procedures in place to detect and react to instances of misconduct when they occur, including incident-reporting hotlines, other defined reporting channels, and procedures for investigating allegations and disciplining wrongdoers. Ideally, such policies and procedures will give employees and business partners confidence that they can report known or suspected misconduct internally and that the company will promptly, consistently, and responsibly address the issue. In that case, most allegations might not come to the attention of regulators at all, unless the company decides to make a voluntary disclosure. And if the regulators ultimately learn about the conduct through a voluntary disclosure or otherwise, the company can point out that its compliance program successfully detected—or likely would have detected—the issue, triggering a thorough internal investigation and adoption of any necessary remedial measures. Even when a company first learns about an allegation of misconduct from a regulator, robust investigation and discipline policies and procedures can help a company respond quickly by escalating the issue to an appropriate authority within the company, thoroughly investigating it with assistance from external counsel if necessary, disciplining any involved employees, and implementing other remedial measures to prevent similar misconduct in the future.

As with preventive controls, it is important for a company to develop and document appropriate, written policies and procedures for detecting and addressing misconduct. For example, the regulators might believe that a company is not truly interested in detecting misconduct if it does not make an anonymous incident-reporting channel available to its employees and business partners and inform them of that channel regularly. Similarly, investigation and discipline policies that do not require escalation of serious corruption allegations to senior management or the Board of Directors could suggest that the company is not serious about addressing corruption. The details of every investigation should be memorialized in writing, regardless of the findings, including a detailed description of the allegation, the steps taken to investigate it, factual findings and legal conclusions, and any resultant disciplinary or remedial actions. A formal, consistent, and documented internal process for addressing allegations of misconduct might enable the company to limit the scope of the government investigation by instilling the regulators with confidence that the company can address the issue appropriately.
Procedures for Cooperating with Regulators

When the government initiates an FCPA investigation, it often seeks to induce the subject company to cooperate in exchange for the prospect of future leniency when the regulators consider charging decisions, settlement offers, or sentencing recommendations. Cooperation can demonstrate that the company is sincerely interested in taking responsibility for any misconduct and build credibility that opens the door for negotiating reasonable limitations on the scope of the investigation. In contrast, refusal to cooperate can engender suspicion and make it seem that the company has something to hide, which can result in an expanded and more aggressive investigation. But cooperating with the authorities is not without risk, and companies should consider how to guard against potential pitfalls before they find themselves under investigation.

Cooperation typically entails providing requested information to the regulators, accepting regulators’ input regarding the direction and scope of the company’s internal investigation, and sharing the results of that investigation. It is of critical importance that any information provided to the regulators be accurate and complete. To that end, the company should take steps to ensure that those with relevant knowledge review any information being provided to the government for accuracy and that a designated point-of-contact, typically outside counsel, facilitates the provision of any information. Having multiple individuals respond to government requests for information without a review process in place risks provision of inconsistent, incomplete, or inaccurate information.

Further, the government may request privileged materials or work product, and providing such information likely waives any applicable protections. This could mean, for example, that an otherwise privileged and potentially damaging investigation report provided to the government could be discoverable in subsequent lawsuits filed by competitors, clients, or shareholders. Accordingly, companies must have procedures in place to carefully review all potentially protected materials provided to the government and should carefully consider whether to withhold or provide protected materials. Although waiving privilege and the work product protection might further demonstrate the company’s commitment to cooperation and build goodwill with regulators, DOJ policy prohibits conditioning cooperation credit on a waiver.

External Communications Plan

Finally, companies should have policies and procedures in place, including a crisis communications plan, that govern communication with external parties in case it becomes publicly known that they are under investigation. Clients and shareholders that learn about an ongoing investigation will likely want to know how the company is handling the matter and what the outcome might be. High-profile investigations might trigger media inquiries. By establishing policies and procedures for responding to inquiries and engaging external stakeholders before a crisis arises, the company can quickly provide information and demonstrate that it is addressing the situation in an appropriate and responsible manner, thereby minimizing damage to its
reputation. As with communicating with regulators, external communications should be funneled through a single point-of-contact, such as a member of senior management or a company spokesperson, to ensure that the message is consistent, and counsel familiar with the investigation should be consulted to ensure that all information is accurate and that no privileged information or work product is inadvertently disclosed to third parties. In light of today’s regulatory environment, it is not unheard of to have an outside “crisis communications advisor” waiting in the wings should a problem arise. Many companies conduct “beauty contests” in order to compare and evaluate the different offerings and approaches of such experts.

* * *

Recent FCPA enforcement history shows that no company, regardless of the strength of its compliance program, is invulnerable to investigation for the misconduct of its employees. Accordingly, responsible companies should anticipate that they may be subject to a government investigation at some point in the future and take proactive steps to prepare for that possibility. Although any government investigation is likely to consume substantial time and resources and may undermine a company’s reputation, those impacts can be mitigated by having an appropriately designed and well-documented compliance program in place, as well as policies and procedures for promptly responding to allegations of misconduct, cooperating with the authorities, and communicating with external parties.