



Investigations and the Foreign Corrupt Practices Act

By Ken Yormark
Protiviti Managing Director

As growing numbers of U.S. companies pursue opportunities in the global marketplace, many have encountered ethical situations that have given rise to government investigation of potential violation of the Foreign Corrupt Practices Act (FCPA). Although enacted almost 30 years ago, compliance with the FCPA is once again in the regulatory spotlight – and has many executives and managers in the U.S. and abroad debating whether “getting things done” in countries accustomed to less rigid ethical standards will give rise to action by the Department of Justice (DOJ) and Securities and Exchange Commission (SEC).

FCPA Requirements

Ultimately, managers will need to focus on the disbursement side of the business, with an eye toward meeting the two main principles of the FCPA. First, it prohibits bribes of foreign public officials. Second, it requires accurate books and records and an adequate system of internal controls.

So who is covered under the FCPA? Individuals in the U.S. – including “a person, firm, officer, director and employee” – as well as their agents or other third-party intermediaries are prohibited from paying, offering or promising to pay bribes to foreign public officials, foreign political parties and their officials, and any candidate for foreign political office in order to obtain, retain and/or direct business. It is important to note that payments to facilitate or expedite the performance of “routine governmental action” are specifically excluded. This anti-bribery provision was extended in 1998 to foreign firms and persons who “act in furtherance of such a corrupt payment” within the U.S. and its territories. The Act’s accounting provisions are applicable to companies that list their securities in the U.S.

Over the last several years, government prosecution of FCPA cases has increased, and there is no telling how many cases may have been settled out of court. The SEC and the Department of Justice have clearly signaled that neither “willful ignorance” nor improper activity will be tolerated and that companies must have internal controls in place to evaluate, mitigate and monitor their FCPA risk.

For example, the SEC and Tyco International Ltd. reached a \$50 million settlement in April 2006 to close the investigation, which began in 2002, of certain accounting practices. The SEC had alleged that Tyco subsidiaries in Brazil and South Korea had made improper payments to government officials in connection with obtaining contracts. In its settlement, Tyco didn’t admit or deny the charges, but its chairman and CEO issued a statement noting, “This investigation was one of several legacy matters inherited by the current management team as a result of alleged wrongdoing on the part of previous management.” Among the changes that Tyco’s new management made to improve transparency was to double the size of the audit staff to provide accurate and independent oversight of financial reporting, and to require all its 250,000 employees worldwide to be certified annually under a comprehensive Guide to Ethical Conduct.

Begin with Basics

While FCPA investigations ultimately will require you to analyze what is being paid out of the organization, it is important to first consider the context in which your company conducts business. Do you operate in countries with a high risk for corruption? Have third-party agents, sub-agents or other intermediaries been used? How much market share do you own? Have there been efforts to “break into” new markets?

Next, consider the entity-level programs and controls designed to help mitigate your FCPA risk. How thorough were the due diligence procedures when entering into joint venture or agent agreements? Did your anti-fraud, anti-bribery and/or FCPA policy adequately address your company’s position on these issues, and further, were they effectively communicated within your organization? Were these policies, procedures and ethical business practices affirmed, or certified – and by whom? Was ethics and/or compliance training provided within the organization and did it address FCPA issues? Who participated in this training program? What protocols have been used by employees to obtain advice about requests for “payments” or “gifts” in-country? Did the terms of your agreement with business partners reinforce your commitment to FCPA compliance? Most importantly, how have these programs and controls been monitored?

Red Flags - Probing Numbers and People

Once you have completed review of those items above, you can then focus on specific subsidiaries and look for payments that do not make sense. There can be payments to consultants and agents for “intangible” services. For example, if there is an invoice for \$100,000 worth of services rendered, you would have to ask: How do I know these services took place? What did they actually do for the company? If there is no tangible product to review, how does a company know if it received \$100,000 worth of services or if it was a political payoff?

This is a starting point to probe deeper. Ask people within the organization: What was the benefit of this particular payment? Can I see where that benefit took place? Also, look at this with a broader perspective. Compare your company’s payment in a particular place to what is the norm in your industry. Of course, the investigation would extend to the contractor that did the work. What services did they do and can they produce time sheets for the people who did the work?

Most importantly, federal regulators – as well as a company’s external auditors – will immediately want to know who within the company was involved in the transaction in order to determine whether the matter at hand represents a “one-time” event or more pervasive and systemic breakdown of internal control. Who authorized the offer of a bribe or actual payment of one? Who else knew about it but deliberately ignored the matter or simply looked the other way? How many payments were made and over what period? Was there an attempt to disguise the nature of the payment? Has this activity occurred in more than one location?

Documentation is a key area of inquiry. As part of the FCPA, companies need to maintain proper documentation and proper accounting records based on Generally Accepted Accounting Principles. If a company is doing its own internal probe, investigators would be very concerned if a substantial amount of documentation for certain transactions cannot be produced. The unavailability of documents and the lack of details about a service are red flags that can prompt the federal government to do their own investigation.

When documents can be located, investigators turn to the next question: Do the numbers make sense?

Here is a simplified hypothetical example. A company purchases 100 pounds of rice at a dollar a pound. If this company is in the business of repackaging and reselling the grain, I would expect to see sales in connection with that purchase. Let's say the 100 pounds translates into 1,000 packages of grain that go to various groceries. If I see that purchase results in fewer packages, I know there is a problem. If the economics do not make sense, there is a good chance there might be a second set of accounting records that reflect what actually happened.

Another red flag would be if the company is paying twice what the market pays for grain. Whether the purchase concerns the tangible commodity of our example or the intangible services of the contractor, investigators are likely to find some way in which the cost factors or the ratios or some other factor in the equation do not make sense.

Understand Disbursement Spending

While computer-assisted audit techniques – including forensic data analysis – are essential in understanding the disbursement spend for FCPA investigation purposes, these same activities can greatly strengthen your ongoing monitoring capabilities. By using electronic tools to routinely analyze disbursement data, companies can identify unusually large or inconsistent payments more quickly. They can help flag unusual travel expenses, such as frequent business trips to the same location, or significant entertainment charges. (One of the SEC's allegations about Tyco's South Korean subsidiary was that it provided entertainment to government officials.)

While helping to detect potential FCPA compliance violations, ongoing monitoring activities also serve as an effective deterrent – when employees know that somebody is monitoring them, their behavior naturally tends to fall more within the expected norm.

Re-evaluation of risk exposure also should be constant. Geopolitical realities may ratchet up a company's risk; when that happens you need to determine how to prepare and protect your company.

Assessing FCPA Risk

To help understand its potential exposure related to non-compliance with the FCPA, a company's risk assessments activities should include consideration of fraud and misconduct – and specifically, common fraud scenarios involving the FCPA. Fraud risk assessments, or more targeted FCPA risk assessments – can “stand-alone,” or be incorporated as a module within an organization's enterprise risk assessment. Other techniques can be used to help identify potential FCPA risk, including (but not limited to): internal discussion or interviews, document review, surveys and data analysis.

The identification and measurement of fraud and related FCPA risk enables organizations to help identify potential improvement opportunities within their system of internal control. Oftentimes this reveals potential FCPA violations that need to be further investigated, or even self-disclosed to federal regulatory agencies.

The proactive approach of making a voluntary disclosure to federal regulators can benefit organizations during a sometimes very difficult – and distracting – time. When a company steps forward and reports on what they plan to do to remediate the situation, regulators have historically viewed this in a positive manner – resulting in the reduction of potentially disruptive government action and penalties.

Employee Education and Awareness

In order for organizations to help mitigate their FCPA risk, it is absolutely critical to educate employees about the provisions of *Foreign Corrupt Practices Act* and the company's corresponding compliance policies and procedures. Oftentimes, violations occur simply because employees were not aware that what they were doing was wrong.

Due to challenges posed by geography, operations, culture and language, there is no single way to best educate employees and agents. Companies are now taking a "multi-method" approach to the delivery of education and awareness programs, including in-person, CD-ROM and Internet-based training provided in different languages. Messages are then reinforced through the distribution of informational packages, annual certifications and performance reviews. To broadcast the message even more widely, a company might send e-mail, post notices in a common area such as a coffee room or on its intranet or include a printed message on (or with) pay stubs or in newsletters. Managers have to think creatively about how to reach the rank-and-file employee, who may or may not have access to internal computer communications.

Nonetheless, it is the responsibility of management and the board of directors to make sure the message is received by everyone within the company and those conducting business on its behalf – from the secretary and the security guard to the worker on the loading dock. Top executives have a special responsibility to set that tone. Why would middle managers be motivated to abide by the FCPA requirements if they sense upper managers are not particularly concerned?

Another highly important aspect of this internal education campaign is to have the effort reinforced by an outside party such as a legal or consulting firm. Bringing in outside advisers sends a strong message from upper management: "We are so supportive of this process that we are bringing in an outside organization to help educate us, so we will all understand it and abide by it."

Having that outside presence involved in education, as well as the investigation, can set the stage for potential changes in business practice. Once management is provided with information about control gaps, risk exposure and even potential violations, the company may have to make an educated – but tough – business decision. They may have to tell a subsidiary that they are not going to do business the way they have done it in the past, and that can be detrimental for a time. A company might not be able to get the same contracts or vendors, or it may have to spend a little more money with traditional vendors.

That can be hard medicine to swallow. But again, if a company has been working with an independent investigator, federal regulators will take notice of the company's commitment to change. An outside party helps to confirm that a company's investigation was truly independent. If a company has been aggressive in its self-scrutiny and presents its findings to the Department of Justice and/or SEC – along with a robust remediation plan – it is likely that they will have a more successful negotiation regarding potential civil and criminal action.

Ken Yormark is a Managing Director in Protiviti's Business Risk practice where he heads the Financial Investigations and Sarbanes-Oxley Anti-Fraud initiatives. Ken has more than 20 years of experience in the areas of forensic and investigative services, having managed and conducted hundreds of complex – and often high profile – financial investigations involving major corporations, noted law firms, and government agencies.

Article from Protiviti's KnowledgeLeader – www.knowledgleader.com

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.