Paying Bribes Abroad Will Get You in Hot Water in the US

Brian M. Gaff, Stephen G. Huggard, and Gregory W. Carey
Edwards Wildman Palmer LLP

Because of its broad and ambiguous language, the US Foreign Corrupt Practices Act prohibits much more conduct than most people might think.

The US Foreign Corrupt Practices Act is an extremely broad federal law focused on preventing corrupt business activity that impacts every company doing business abroad.

A recent survey of corporate compliance officers revealed that the Foreign Corrupt Practices Act (FCPA), the US law that prohibits the paying of bribes in connection with certain foreign business transactions, is one of the top five things keeping them up at night—and for good reason.

There's a steady flow of reports of the government extracting millions of dollars in penalties from companies for bribes paid by their employees or agents. Additionally, recent front-page stories about Wal-Mart allegedly paying bribes to fast-track the construction of stores in Mexico and the company's public disclosure that its internal investigation into the allegations cost upwards of $100 million in just one year has sent shivers through the business community.

Given its international nature, every company in the computing industry—from hardware manufacturers to component suppliers to companies seeking patents outside the US—must ensure they're doing all they can to comply with the FCPA, especially given the demand for computer technology and services in many countries that are hotbeds of corruption.

Visit the IEEE Computer Society's website for the podcast that accompanies this article (www.computer.org/portal/web/computingnow/computing-and-the-law).

WHAT IS THE FCPA?

The US Congress enacted the FCPA in 1977. The legislation was a response to SEC investigations revealing that hundreds of US enterprises—including many of the country's most admired companies—had paid hundreds of millions of dollars to foreign officials and political parties to obtain government contracts, gain access to lucrative markets, and impact foreign elections.

In general, it's a crime under the FCPA for US persons and companies, certain issuers of securities in the US, and foreign persons in the US to make a corrupt payment, directly or indirectly, to a foreign government official for the purpose of obtaining or retaining business.

Because of the law's broad and
ambiguous language, however, the FCPA prohibits much more conduct than most people might think:

• It’s a crime to give or offer anything of value, including cash, gifts, political contributions, travel expenses, and so on, in exchange for a business advantage. A crime is committed even if the bribe is unsuccessful.
• A payment—regardless of the amount—will be considered corrupt if the payer’s intention is to influence a foreign official’s decision-making, cause him to influence the decision of a governmental body or agency, induce him to do or not do something that violates his duties, or obtain an advantage over other companies.
• Companies can and will be held liable for the violations of their employees—even if the employee was not high ranking or was specifically instructed not to engage in the improper conduct.
• Companies that use third parties such as brokers and other agents to sell their products abroad will be liable in the event those third parties make improper payments to generate business for the company.

Therefore, it’s imperative for companies to fully vet and monitor those working on their behalf to prevent “rogue agents”—who care more about their commission than complying with US law—from potentially subjecting the company to enormous harm.

**WHO EXACTLY IS A “FOREIGN OFFICIAL”?**

Another dangerous ambiguity of the FCPA is that it doesn’t fully define exactly who is considered a “foreign government official.” An officer or employee of a clearly defined agency of a foreign government is undoubtedly a “foreign government official.” Unfortunately, any clarity ends there, because the FCPA also prohibits corrupt payments to the officers and employees of “instrumentalities” of foreign governments, and Congress didn’t define that term in the FCPA.

Whether an entity is an “instrumentality” depends on the facts and circumstances of a particular scenario—the key factors being the level of government ownership or control and whether government officials are in prominent positions.

**GIFTS, TRAVEL, AND ENTERTAINMENT EXPENSES**

Companies struggle on a day-to-day basis with how to deal with the giving of gifts and the payment of travel and entertainment expenses to foreign officials. While there’s no bright line test, the government has provided some guidance on what types of payments are permissible—so long as there’s no corrupt motive for the payment.

Recognizing the practicalities of the business world, the government has acknowledged that local culture often necessitates the giving of gifts and offering hospitality as signs of respect that won’t influence a person to act one way or another. The government also recognizes that it’s often appropriate for companies to give gifts and pay certain expenses in the normal course of carrying out a business relationship.

While every situation is different, the government has provided some helpful guidance on what types of payments are presumptively permissible. For example, paying a moderately priced bar tab in connection with a business meeting or conference would be appropriate, while taking foreign officials to a lavish dinner would not. Similarly, it would likely be appropriate to pay the expenses for a foreign official to travel to inspect a manufacturing facility that had a connection to an actual or potential business relationship, but it would be inappropriate to provide the official first-class accommodations and turn the business trip into a leisure excursion. Likewise, giving a moderately priced vase as a wedding present to a foreign official who heads an entity with which a company does business would probably not violate the FCPA, but an unnecessarily expensive gift would suggest a corrupt intent. The devil, as they say, is in the details.

Where exactly the line falls depends on the facts and circumstances of a given case, and
companies must be wary that the government might not ultimately agree with where they decided to draw the line.

**BEWARE OF THE WHISTLEBLOWER**

Recent changes in the law provide incentives for employees and others to “blow the whistle” to the government in the event they come across FCPA violations. Specifically, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2011 created a bounty program for whistleblowers who voluntarily provide original information to the Securities and Exchange Commission. That bounty is between 10 and 30 percent of the penalty the government ultimately collects based on the tip. Moreover, most whistleblowers aren’t required to first report the matter to their employer.

As a result of Dodd-Frank, it’s imperative that companies encourage their employees to deal with matters internally so they can discover and address potential violations before the government becomes involved.

Among other things, companies want to avoid scenarios in which a “trigger-happy” employee with selfish motives—such as a big payday—or a grudge provides misleading information to the government or is simply mistaken about the facts he reports, in which case the company might needlessly have to endure the cost and distractions of a government investigation.

**THE NEED FOR A COMPLIANCE PROGRAM**

Given the increasing emphasis on FCPA enforcement, having a specific FCPA compliance policy is the “new normal.” Every company with international exposure must have a compliance program in place that reinforces anticorruption standards and takes steps to prevent violations from occurring.

Responding to violations, conducting internal investigations, and cooperating with government investigations can generate an enormous expense. Not only can legal costs be immense, but an investigation is a distraction to senior management. In addition, a company could suffer reputational harm in the event actual or potential FCPA violations are publicly disclosed.

If a violation does occur, one of the first things the government will look at when determining how to handle a particular incident is whether the violator took its compliance obligations seriously and had a policy in place to prevent violations. FCPA compliance programs will vary from company to company, but the cornerstones of an effective compliance program must include:

- clear policies and procedures;
- a demonstrable commitment to FCPA compliance by company management;
- adequate resources to actually implement the program;
- a thorough risk assessment of all markets where the company operates;
- training of employees and agents;
- setting up internal control mechanisms to detect violations;
- appropriate disciplinary measures for violators;
- mechanisms for vetting third parties, such as brokers, that act on the company’s behalf;
- internal reporting mechanisms, such as confidential hotlines; and
- regular review and updating of policies and procedures.

The US government is devoting increasing resources to investigating and prosecuting FCPA violations. This trend will continue as whistleblowers tee up cases for the government to take a swing at.

Given this regulatory environment, every company that does business abroad must have an FCPA policy—often designed by a lawyer with FCPA expertise—that has teeth, and each must demonstrate an actual commitment to preventing violations. As the saying goes, an ounce of prevention is worth a pound of cure.

Brian M. Gaff is a senior member of IEEE and a partner at the Edwards Wildman Palmer LLP law firm. Contact him at bgaff@edwardswildman.com.

Stephen G. Huggard is a partner at Edwards Wildman Palmer. Contact him at shuggard@edwardswildman.com.

Gregory W. Carey is an associate at Edwards Wildman Palmer. Contact him at gcarey@edwardswildman.com.