

CORPORATE COUNSEL

Oh, That Money ... I Don't Know, It Just Crawled Into My Hand!

John C. Kocoras

American companies are being bombarded with warnings about the federal Foreign Corrupt Practices Act (FCPA), and the warnings have become increasingly ominous.

In November 2009, the head of the Department of Justice's (DOJ) Criminal Division specifically advised pharmaceutical companies that prosecutors are focusing on their industry. Commentators previously suggested that the DOJ treats FCPA concerns as second only to national security concerns, but in February 2010, a prosecutor who supervised FCPA matters at the DOJ stated at a conference that corruption is a national security issue.

The U.S. is not alone in its heightened focus on international bribery. In April 2010 the United Kingdom enacted the Bribery Act 2010, which makes investigating international bribery a law enforcement priority in the U.K. Just as U.S. authorities have made clear that U.K. companies with U.S. operations must heed the FCPA, U.S. businesses with U.K. operations are well advised to closely review internal measures to comply with the Bribery Act.

This article underscores the hazards companies face in securing business overseas, focusing on the risks of shell companies used to facilitate bribes. It also outlines simple and concrete steps that can be taken to minimize the risks of violating the FCPA or the U.K. Bribery Act through payments to shell companies.

PROHIBITIONS ON INTERNATIONAL BRIBERY IN THE U.S. AND THE U.K.

The FCPA generally prohibits corrupt payments to foreign officials for the purpose of obtaining or keeping business, including payments made by a company's third-party agents. 15 U.S.C. § 78m et seq.

In addition to anti-bribery provisions, the FCPA also contains accounting provisions that generally require companies with securities listed in the U.S. to keep books and



John Kocoras

records which accurately reflect transactions and to maintain an adequate system of internal accounting controls. Id.

But, in essence, FCPA actions are about bribery, even in cases where the government only charges easier-to-prove violations of the accounting provisions.

While the U.K.'s Bribery Act does not contain separate accounting provisions, in some respects it imposes greater anti-bribery restrictions than the FCPA, reaching bribes that are intended only to influence private actors, not just public officials. The Bribery Act generally imposes liability on corporations for failing to prevent bribes by a person performing services for the corporation, again including third-party agents.

Notably, however, the Bribery Act provides that a company can avoid liability if it had in place "adequate procedures" designed to prevent persons associated with the company from paying bribes.

THE CHALLENGE OF 'ADEQUATE PROCEDURES' TO PREVENT EVOLVING METHODS

Of course, the "adequate procedures" defense is inherently problematic — for the defense to be adjudicated, the "adequate" procedures must have failed to prevent some instance of bribery. Traditional procedures to prevent bribery have included tightened accounting controls and global training.

A constant challenge, however, is that

despite these efforts, employees and agents dealing with foreign officials regularly perceive a wink and a nod from management to take all necessary — and in some cases customary — steps to meet sales targets. With a limited ability to eliminate the motive and opportunity to pay bribes, companies are often left to combat the means of paying bribes.

Mechanics of bribe payments have evolved substantially, developing from cash stuffed in a suitcase and vacations falsely characterized as business trips to intricate, multinational wire transfers from account to account across the globe. Without understanding how these bribes are actually paid, it is nearly impossible to detect and prevent them.

As recent FCPA cases illustrate, the most popular way to get money from a corporate bank account into the hands of a corrupt foreign official might be through payments to intermediary shell companies. These shell companies typically purport to provide services in connection with the foreign business, but the services they identify are meant to be difficult to verify.

Using shell companies appeals to bribe payers because the funds are drawn from the same corporate accounts as funds for legitimate payments, and they exit those accounts in the same manner as legitimate payments. As a bonus, the bribers can inflate the payments to skim a little something off for themselves, or to easily compensate others who assist.

Corrupt officials receiving payments favor the shell company approach because someone examining the officials' own accounts will at most see only the payment from the shell company, not a party with a government contract. Additionally, despite increased international cooperation, tracing such payments to their original sources remains cumbersome, particularly when payments are routed through a chain of banks including ones in countries with tight bank secrecy.

Recent cases discussed below illustrate

the use of shell companies to facilitate bribes, followed by a list of steps to create an environment designed to detect and prevent corrupt payments.

SHELL COMPANY INTERMEDIARIES VIOLATING THE FCPA

In *United States v. Antonio Perez*, defendant Antonio Perez, a former controller of a U.S. telecommunications company, pleaded guilty in April 2009 to conspiring to violate the FCPA by arranging for bribes to officials of Telecommunications D'Haiti, Haiti's state-owned national telecommunications provider.

Telecommunications D'Haiti, the sole provider of landline telephone service in Haiti, contracted with international telecommunications companies to allow those companies' customers to call into Haiti. Telecommunications D'Haiti charged a set rate for each minute of calls.

According to court documents, the president of Perez's telecom company sought an intermediary's help in bribing Telecommunications D'Haiti officials. The intermediary established a shell company in Haiti, JD Locator Services, Inc.

JD Locator Services, Inc.'s sole purpose was to hold a business bank account into which payments would be made by Perez's company and two other U.S. telecom companies, with the payments ultimately destined for officials of Telecommunications D'Haiti. The three U.S. companies hoped that the bribes would lead to preferred rates and credits for certain amounts they owed.

Records indicate that the U.S. companies wired over \$1 million to the JD Locator Services, Inc., account, with approximately \$955,000 of that passed as bribes. Perez's company characterized payments as fees for "consulting services," while JD Locator Services, Inc., recorded them as "commissions."

Similarly, in *United States v. Latin Node, Inc. (Latinode)*, the government indicted Latinode for violating the FCPA by bribing Honduran and Yemeni officials for telecommunications contracts and favorable rates. In April 2009, Latinode entered a plea agreement committing to pay a \$2 million fine.

U.S.-based Latinode provided wholesale telecommunications services using internet protocol technology. Latinode caused a subsidiary to enter into a purported "consulting" agreement with another company, which in turn entered into a purported "consulting" agreement with a Honduran company owned in part by a Honduran official. Two days after

Latinode secured the contract, its subsidiary paid the official's company \$100,000, followed by \$200,000 the next day, all as "consulting" fees.

In 2008, Faro Technologies, Inc., entered into a two-year non-prosecution agreement with the DOJ and settled an enforcement action brought by the Securities and Exchange Commission by paying a \$1.1 million criminal fine and a \$1.85 million civil disgorgement penalty.

Faro, which develops computerized measurement devices for a variety of industries, reportedly paid Chinese officials nearly \$450,000 in bribes disguised as "referral fees" to secure contracts worth nearly \$5 million. Internal e-mails reveal that, like the companies above, Faro tried to avoid exposure by making payments through a shell company.

In 2007, Paradigm B.V. entered into a non-prosecution agreement and agreed to pay a \$1 million penalty for FCPA violations.

Paradigm, a Netherlands company with operations in Houston, Texas, provides software to the oil and gas exploration industry. Paradigm acknowledged that it deposited \$22,500 into a Latvian bank account of a British West Indies consulting company recommended by an official of Kazakhstan's national oil company, KazMunaiGas, after Paradigm secured a contract with KazMunaiGas.

Prosecutors emphasized that Paradigm performed no due diligence investigation of the consulting company, had no written agreements with the company, and did not receive any services from it.

STEPS TO HELP AVOID CORRUPT SHELL COMPANIES

While it is impossible to determine the integrity of all vendors, cost-effective measures can often be implemented to reduce the risk of unwittingly paying shell company intermediaries that facilitate corrupt payments. For vendors whose payments will exceed a specified amount, who are working on a project with significant state involvement, or who are working in jurisdictions where bribery historically has been a problem, the following procedures should be considered:

- Require written contracts, which are to be reviewed by staff outside the chain of command of the sponsor of the relationship.
- Allow the contract reviewer to contact the vendor directly to discuss the services to be performed.
- Require separate written certifications

of compliance with anti-bribery laws of the relevant foreign countries. Consider review by independent counsel when concerns are particularly high.

- Require physical addresses from vendors. In some cases research should be conducted to ensure that the vendor is a brick and mortar operation and the address is not simply a mail drop. This can often be done using electronic databases, although sometimes it might be necessary to have someone visit the address.
- Independently retrieve corporate registration records and other public records including media reports on principals to ensure the vendor has actual operations and no issues of integrity have emerged in their pasts.
- Check individuals' names against commercial databases listing 'Politically Exposed Persons.'
- Insist on audit rights where appropriate, and exercise those rights when suspicions of bribery arise.
- Insist that vendors provide written descriptions of services to be provided and demand detailed invoices describing services performed and associated expenses.
- Remit payments to accounts only in countries where the vendor is operating or is based.
- Require an accountable employee such as a project manager to verify that specified services were provided before payment is made.

While there is no guarantee that any measure will prevent an illegal payment, an array of procedures, when combined with anti-corruption policies and training, will foster a culture of compliance designed to stop illegal bribes made through shell companies before they are ever made. They will also deter would-be embezzlers. And importantly, as a last resort, they will bolster a defense if law enforcement authorities come calling.

John C. Kocoras, a partner in the law firm of McDermott Will & Emery, is a former federal prosecutor and managing director of a global investigations company and focuses his practice on complex investigations and white-collar criminal defense issues. He is based in the firm's Chicago office.