Preliminary Communication
UDC 005.7(73)

Jonathan S. Abernethy

U.S. CORPORATE GOVERNANCE AND COMPLIANCE IN AN INCREASINGLY CHALLENGING REGULATORY ENVIRONMENT

Abstract

Increased regulation and well-publicized corporate scandals in the U.S. have caused boards of directors and management to focus more and more on legal and regulatory oversight. Companies today face two particular regulatory challenges. First, there is the U.S. Foreign Corrupt Practices Act (FCPA), which, broadly speaking, prohibits bribery of non-U.S. government officials and has a wide jurisdictional reach. Second, whistleblower provisions of the recently enacted Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") enable company employees and former employees to recover potentially huge bounties for reporting corporate misconduct. This paper examines these two regulatory challenges and ways in which companies can institute and augment compliance programs to mitigate the risks they pose.

INTRODUCTION

The U.S. has well-developed developed corporate governance standards based on concepts such as financial transparency, disclosure of material events, sound risk management, proper internal controls, and independence of a majority of the corporation's board of directors. Corporate governance standards in the U.S. have existed for approximately 150 years, when the New York Stock Exchange first adopted rules for the issuance of regular financial statements, quarterly earnings announcements, and independent audits of a company's financials.[1]

At their core, corporate governance standards for U.S. public companies are designed to protect shareholders. The overarching objective of boards of directors is to maximize long-term shareholder value. However, due to well-publicized scandals such as Enron and WorldCom, and increasing regulation over the past decade, boards must now focus far more on legal and regulatory oversight that they did previously.[2]

This paper examines two challenges in particular that U.S. companies face in this increased regulatory environment: the challenges facing multinational companies in ensuring compliance with the FCPA and the challenges to companies posed by the whistleblower provisions of the Dodd-Frank Act. In light of these challenges, and because of regulators' ever-increasing focus on corporate wrongdoing, boards of directors and corporate management will likely need to spend even more time on legal and regulatory oversight, and, in particular, overseeing compliance programs, in the future.

OVERVIEW OF THE FOREIGN CORRUPT PRACTICES ACT

The Foreign Corrupt Practices Act, or FCPA, is a statute that prohibits bribery of "foreign officials" (non-U.S. government officials) for a commercial advantage.[3] More specifically, the FCPA prohibits corrupt payments or offers to pay money or anything of value to such officials or to third parties acting on their behalf, when such payments or offers to pay are made to assist in obtaining new business or retaining existing business. The term "foreign official" has been interpreted very broadly and may include, among other people, employees of state-owned or controlled entities; advisors or other persons acting on behalf of a government; party officials or candidates for political office; customs officials; and relatives of government officials. Those potentially subject to civil and criminal sanctions under the FCPA include companies whose securities are traded on U.S. stock exchanges and their subsidiaries; U.S. citizens, nationals, and residents; and, under some circumstances, foreign corporations and citizens of other countries.

---

[1] *Report of the New York Stock Exchange Commission on Corporate Governance* (September 23, 2010), at p. 1, available at http://www.nyse.com/pdfs/CCGReport.pdf.
[2] *Id.*at p. 16-17.
[3] 15 U.S.C. § 78dd-1 et seq.

In addition to the anti-bribery provisions of the FCPA, the FCPA contains accounting and internal controls provisions that, in essence, require U.S. public companies and foreign companies listed on U.S. stock exchanges to maintain accurate books and records and to have sound internal controls.[4]

The FCPA imposes harsh penalties on companies. Criminal violations of the anti-bribery provisions can lead to up to $2 million in fines for each violation. For violations of the accounting provisions, the fines can be up to $25 million per violation. In addition, the SEC may seek disgorgement of profits generated through corrupt payments. Companies may also be subject to debarment from government contracts for violating the anti-bribery provisions of the FCPA.

RECENT ENFORCEMENT OF THE FCPA

The last few years have seen a significant rise in enforcement of the FCPA by U.S. prosecutors and regulators. The U.S. Department of Justice ("DOJ") enforces the FCPA's criminal law provisions, while the U.S. Securities and Exchange Commission ("SEC") is responsible for non-criminal enforcement. Since December 2008, there have been eight settlements by corporations each with more than $100 million in combined civil and criminal fines, and five of those eight settlements had fines in excess of $300 million.[5]

Many if not most of the recent FCPA enforcement actions brought by the DOJ and SEC have involved so-called "third-party payments." As noted above, corrupt payment need not be made directly to a foreign official to violate the FCPA. Companies are equally liable if they utilize an intermediary such as a middleman or an agent to make such a payment. Among the most common scenarios is the use of third-party intermediaries such as business consultants or vendors to make payments to foreign officials. In these cases, payments made by the company to the business consultant are often accompanied by invoices with a vague or entirely absent description of services. In other instances, sales agents or vendors are used to pass on payments to foreign officials. In any situation involving the use of third-party intermediaries, a company can be liable under the FCPA if it knew a payment was being passed along to a foreign government official or if was aware of a "high probability" that the payment was being made and "consciously avoided" confirming this fact.

---

[4] 15 U.S.C. § 78m.

[5] The FCPA Blog, "Top 10 FCPA Enforcement Actions," last published April 8, 2011, available at http://www.fcpablog.com/blog/2011/4/8/jj-joins-new-top-ten.html.

Another significant recent trend of FCPA enforcement is the DOJ and SEC's targeting of non-U.S. companies. Of the ten largest FCPA fines imposed upon companies to date, eight have been against non-U.S. companies.[6] A non-U.S. company is subject to the jurisdiction of the FCPA if it lists its shares on U.S. exchanges. But the FCPA also subjects non-U.S. companies to liability for any acts committed in furtherance of a violation "while in the territory of the United States."[7] Although this provision on its face appears only to cover a non-U.S. company's acts while *physically located* in the U.S., the DOJ takes the view that there is jurisdiction whenever a non-U.S. company merely *causes* an act to be done within the territory of the U.S. by any person acting as that company's agent. Thus, for example, under the DOJ's expansive view, payments in furtherance of a bribery scheme made from one non-U.S. bank to another non-U.S. bank that merely pass through a correspondent U.S. bank could be sufficient to confer jurisdiction under the FCPA. The DOJ's expansive view has not yet been successfully challenged in court.

The FCPA's reach may also be extended to non-U.S. companies and employees by theories of liability such as conspiracy and aiding and abetting. Employees may face criminal liability even if they did not directly participate in bribery, were not the leaders of a bribery scheme, and did not know whether or how specific bribes were being paid. Conspiracy and aiding and abetting charges can be used to impose liability on actors who have no connection to the U.S. as long as they assist other actors in a scheme and those other actors have a U.S. connection.

FCPA AND ANTI-CORRUPTION COMPLIANCE

The increasing aggressiveness of U.S. authorities in enforcing the FCPA has led numerous companies to establish anti-corruption compliance programs or to augment existing compliance procedures. Among the many steps companies have taken is to establish due diligence procedures to ensure that their agents, middlemen and business partners are acting in compliance with the law and that the transactions companies engage in do not have corruption risks.

In conducting due diligence, companies with operations overseas must be attuned to FCPA "red flags," or examples of conduct that could suggest corrupt payments are being made. Red flags include unusual or excessive commission or payment requests by third-party intermediaries, retention of third-party intermediaries or joint venture partners who were recommended by government officials, an apparent lack of qualifications on the part of a the third party, a refusal by the third party to certify that it will not take any action that might cause a violation of the

[6] *Id.*
[7] 15 U.S.C. § 78dd-3(a).

FCPA, and a lack of transparency in expenses and accounting records on the part of the third party.[8] Companies must also be attuned to increased risks in areas of the world that have a history of corruption. The most widely-regarded indicator of such corruption "hot spots" is the annual Corruptions Perception Index by Transparency International, which ranks countries based on their perceived levels of corruption.[9]

In addition to due diligence, many companies have taken extensive steps to train their employees on the FCPA and particular corruption risks in their industry sector. FCPA compliance policies also routinely contain detailed procedures for authorizing, approving, and reimbursing gift, travel, meal, and entertainment expenses involving foreign officials. Such gifts, travel, meals and entertainment are "things of value" under the statute that, if given corruptly, can cause a company to be in violation of the FCPA. In addition, FCPA compliance programs often require employees to certify on an annual basis that they are unaware of any bribery or accounting and internal controls violations, or, if they are aware of such violations, to describe the conduct in question. These procedures allow companies to investigate potential violations and remediate them where necessary.

Compliance policies and procedures are a critical for multinationals, given the increasing aggressiveness of U.S. authorities in investigating and enforcing the FCPA and the penalties that can result from a violation. At their most basic level, training and robust compliance programs should decrease the likelihood that employees will engage in conduct that may violate the FCPA. In addition, compliance programs place companies in a better position to avoid prosecution or enforcement actions in the U.S. if their employees ever commit a violation of the FCPA. One of the most important factors that U.S. federal prosecutors consider in the decision whether to prosecute a corporation is "the existence and effectiveness of the corporation's pre-existing compliance program."[10] In addition, senior DOJ officials have emphasized that a company's compliance program is "one of the most important factors" that they consider in deciding whether to bring charges.[11]

Companies with effective compliance programs also are eligible for a significant reduction in criminal fines if they ever do face prosecution under the FCPA. Under the U.S. Sentencing Guidelines, the existence of such a program is a one of two factors that mitigate punishment.[12] The Sentencing Guidelines provide for a reduction in a fine "[if] the offense occurred even

---

8 *See* DOJ's Lay Person's Guide to the FCPA at p. 4, found at http://www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf

9 The Corruption Perceptions Index is available at http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results.

10 Principles of Federal Prosecution of Business Entities, United States Attorneys' Manual § 9-28.300.

11 May 25, 2010 Speech by Acting Deputy Attorney General Gary Grindler to Compliance Week 2010.

12 U.S.S.G. Ch. 8, Introductory Commentary. The other mitigating factor is whether the company self-reports any violation, cooperates in an investigation, and accepts responsibility for its criminal conduct.

though the organization had in place at the time of the offense an effective compliance and ethics program."[13] In the civil enforcement context, among other factors, the SEC will examine whether a company had effective compliance procedures and will give credit in appropriate circumstances for such procedures.[14]

The incentives to institute robust compliance policies are therefore quite significant under the FCPA. But those incentives are even greater for multinationals who conduct business in the United Kingdom, due to the passage of the United Kingdom's Bribery Act, which took effect on July 1, 2011. The most draconian provision of the Bribery Act makes it a crime for companies who do business in the UK to fail to prevent bribery by their employees, agents, and subsidiaries. This is a strict liability provision, meaning that even if a company does not know that one or more of its employees, agents, or subsidiaries are engaging in bribery, it still faces liability. The Bribery Act does contain a defence, however: companies that can prove they had "adequate procedures" in place to prevent bribery will not be liable. Thus, for companies that do business in the U.K., having an effective compliance program in place is the only way to mount a defence to a charge of failing to prevent bribery by their employees, agents, and subsidiaries.

THE DODD-FRANK ACT'S WHISTLEBLOWER PROVISIONS

Another significant challenge for U.S. companies is the whistleblower provisions of the Dodd-Frank Act. These provisions require the SEC to award at least 10 percent and no more than 30 percent of total monetary sanctions to a whistleblower who voluntarily provides the SEC with original information that leads to successful enforcement action with more than $1 million in penalties.[15]

The incentives to recover a potentially huge reward for reporting on misconduct at a company are perhaps most significant in the FCPA context. Given the recent spate of enforcement actions with fines in excess of $100 million, FCPA whistleblowers in the future could receive payments

---

[13] U.S.S.G. §8C2.5(f)(1).

[14] *See* SEC Release No. 44969, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions (October 23, 2001), available at http://www.sec.gov/litigation/investreport/34-44969.htm.

[15] 17 C.F.R. § 240.21F-3. "Original information" is defined as information that is derived from a whistleblower's independent knowledge or analysis and that is not already known to the SEC nor exclusively derived from the media, a judicial or administrative hearing, or a government report. A whistleblower need not have first-hand knowledge of a potential violation to qualify, however; "independent knowledge" may be gained from "experiences, communications and observations" with others inside or outside of a company. Information obtained from a communication subject to the attorney-client privilege is excluded from the definition of original information. In addition, certain categories of employees, including compliance, audit, and legal personnel who obtain information about a potential violation, are generally excluded from obtaining awards. 17 C.F.R. § 240.21F-4(b).

in the tens of millions of dollars. The FCPA is just one area in which a whistleblower may obtain a significant bounty, however. The whistleblower provisions apply to the full panoply of violations over which the SEC has jurisdiction, including insider trading, Ponzi schemes, and market manipulation. The SEC estimates that it will receive approximately 30,000 tips, or reports of potential violations, per year under the whistleblower program.[16]

From a corporate compliance standpoint, the whistleblower provisions pose a significant problem because they do not require corporate whistleblowers to report their allegations internally through existing compliance channels. Thus, companies now face risks that disgruntled employees or former employees will go straight to the SEC with a tip regarding potential misconduct before informing anyone in the company's compliance or legal department. One possible outcome is that highly developed corporate compliance programs that rely on internal reporting may be circumvented. Even more serious, when a whistleblower reports a tip to the SEC and the matter results in an enforcement action or a criminal case, the company in question likely will not be eligible for a reduced fine under the federal Sentencing Guidelines for voluntarily disclosing the potential problem.[17]

The whistleblower rules do provide that a factor that may increase the amount of an award is "whether, and the extent to which, the whistleblower . . . participated in internal compliance systems."[18] Conversely, if a whistleblower interfered with those systems "to prevent or delay detection," or if a whistleblower made a false statement "that hindered an entity's efforts to detect, investigate, or remediate the reported securities violations," the award likely will be reduced.[19]

In addition, the whistleblower provisions contain a "look back provision" for whistleblowers who initially report information pursuant to a company's internal compliance procedures. If the whistleblower submits the same information to the SEC within 120 days of notifying the company, then the whistleblower will be deemed to have provided the information to the SEC on the date he or she first notified the company.[20] This rule protects the original whistleblower if, during this 120-day period, another whistleblower tips the SEC to the same conduct, provided that the first whistleblower's information was specific and credible. The SEC emphasized that this look back provision is designed to support compliance programs "by allowing employees to

---

[16] SEC Release No. 34-64545, Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934 (May 25, 2011), at p. 209, available at http://www.sec.gov/rules/final/2011/34-64545.pdf

[17] See U.S.S.G. §8C2.5(g)(1) (corporation can obtain a reduced fine if, "*prior to an imminent threat of disclosure or government investigation*," it self-reports an offense to "appropriate governmental authorities," cooperates in the investigation, and accepts responsibility for its conduct) (emphasis added).

[18] 17 CFR 240.21F-6(a)(4).

[19] 17 CFR 240.21F-6(b)(3).

[20] 17 C.F.R. § 240.21F-4(c)(3).

take their concerns about possible violations to appropriate company officials first while still preserving their rights under the Commission's whistleblower program."[21]

WHAT COMPANIES CAN DO TO RESPOND TO THESE CHALLENGES

No company can eliminate the risk of an employee committing an FCPA violation. Nor can any company eliminate the risk of an employee or former employee tipping the SEC to a potential violation in hopes of obtaining a whistleblower bounty. But companies can and should consider various steps to deal with the challenges posed by the FCPA and the Dodd-Frank whistleblower provisions.

As an initial matter, and as noted above, companies with international operations should institute robust FCPA compliance programs. These programs should contain, among other things, procedures for due diligence in connection with third party agents, intermediaries and other business partners; employee training; and gift, travel, meal, and entertainment expenses involving foreign officials. In addition, companies should consider instituting several steps to encourage employees or former employees to first report potential violations internally before reporting them to the SEC under the whistleblower program.

First, companies should consider augmenting their employee certification process. As noted above, employee certifications are often used in FCPA compliance programs, and they can be useful in obtaining information from employees about potential violations. In light of the increased risk of whistleblower reports, it may be wise to require employees to certify every quarter or every six months rather than annually. More frequent certifications will increase the odds that a company will learn about potential violations earlier and be better able to address them. This more timely information flow will, in turn, allow companies proactively to investigate issues rather than simply reacting to an SEC request for information about a whistleblower complaint that may ultimately prove meritless. In addition, departing employees should be asked to fill out a certification form asking if they are aware of any conduct in their tenure with the company that might have constituted a violation of the law. Because whistleblowers are often disgruntled *former* employees, companies should have departing employees "go on record" about any potential violations.

[21] SEC Release No. 34-64545, Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934 (May 25, 2011), at 91.

Second, companies should consider enhancing their training of employees on securities law violations. At least in the FCPA context, such training often is a combination of in-person sessions for new employees paired with the requirement that employees periodically view a video training course on their computers. Naturally, video courses have the advantage of training large numbers of employees in a cost-effective manner. But companies should consider conducting more frequent in-person training in light of the risks imposed by the whistleblower provisions. In the end, nothing encourages internal reporting more effectively than when companies show they have an ethical "tone at the top," care about compliance, and take allegations of wrongdoing seriously. In-person training is one way to showcase this commitment to compliance.

Third, companies that have not already established dependable, anonymous channels for employees to report suspected violations should do so right away. Such channels typically take the form of hotlines or email tip-lines where employees can anonymously, and without any fear of retaliation, report on potential legal violations by their colleagues. The hotline or tip-line should be widely publicized to all employees, and any reports of potential violations should be investigated promptly.

CONCLUSION

Companies that establish compliance programs or augment existing programs no doubt will incur costs in doing so. However, the benefits of a robust compliance program outweigh the costs. In the FCPA realm, companies with good compliance programs will reduce the risk of a violation occurring and thereby the risk of potentially huge fines being imposed in an enforcement action. In the whistleblower context, money spent on encouraging employees to report suspected violations internally will be well worth it, compared with the far greater costs of dealing with an SEC investigation initiated by a whistleblower complaint.

As the New York Stock Exchange Commission on Corporate Governance recently observed, "Good corporate governance should be integrated with the company's business strategy and objectives and should not be viewed simply as a compliance obligation separate from the company's long-term business prospects."[22] The challenge for boards of directors and management in the U.S. will be to heed these words amidst a challenging regulatory landscape.

[22] *Report of the New York Stock Exchange Commission on Corporate Governance*, at p. 4, September 23, 2010, available at http://www.nyse.com/pdfs/CCGReport.pdf.