

Global Corruption Enforcement

Protecting Corporate Interests

By Kirk Ogrosky and Jeffrey Hessekiel

For multinational corporations, reducing the risks and concomitant expenses associated with corrupt employee behavior must be a priority. In today's environment, counsel, directors and management must recognize that companies can no longer rely on the mere existence of a compliance program and code of conduct. This article discusses the benefits of embedding compliance doctrine within operations, and how businesses could market integrity and compliance to gain a competitive advantage.

Expansion into markets with challenging regulatory systems poses added risks to companies subject to the Foreign Corrupt Practices Act (FCPA), 15 U.S.C. §§ 78dd-1, *et. seq.* Whether driven through acquisition or organic growth, expansion demands extra attention and expertise by specialized counsel. In 2014, companies should prepare for enhanced U.S. and German enforcement efforts. Mere identification of issues after expansion, however, will be insufficient to minimize risk and deal with enforcement.

The disruption and cost of internal investigations standing alone make counsel with foresight a tremendous value. Over the past decade, the standard practice has been to institute a "letter-of-the-law" compliance program rather than designing integrated compliance protocols that are specific to businesses operations. Unfortunately, many of these compliance programs have left businesses vulnerable to "work around" cultures where operators quickly find ways to avoid compliance processes. For example, if a company sets a monetary limit that requires legal or compliance approval, the company should monitor how many transactions occur right below the limit in ensuing periods.

Notably, almost every multinational business to announce FCPA settlement with the U.S. Department of Justice (DOJ) had a compliance program, code of conduct and Chief Compliance Officer (CCO). This alone should be a forewarning to counsel that it is not enough to have a program in place. Businesses today are better served by moving beyond "compliance programs" to focus on structures that promote and actively market business integrity.

Embedding Compliance

It is evident from dozens of internal investigations, as well as federal criminal investigations and prosecutions, that compliance functions must be embedded within business operations. "Compliance" needs to be internally defined as ethical business practices and the exercise of good judgment. The initial step for counsel, directors, and management is to ensure that an effective compliance program is in place, meaning a program that actively eliminates

opportunities for inappropriate behavior by company employees and third-party contractors. Operations should be incentivized and encouraged to make compliance a part of everyday decision-making. Compliance activities and controls also need to be structured in a way that allows compliance to continually evolve with the business. Companies rely on their general counsels to advise management and boards to ensure compliant cultures and protect assets.

Embedding compliance as part of operations allows for inclusion in real business dynamics, cultivating risk assessment and monitoring, and improvement the allocation of resources. It can also reduce tension between personnel, by repositioning compliance specialists as "best practice consultants" in roles designed to achieve business objectives while assuring the transaction cost of non-compliance are evaluated during execution.

Legal Landscape

For much of the first two decades after President Carter signed the FCPA into law in 1977, DOJ enforcement actions were rare. By the early 2000s, that began to change, and by 2010, dozens of multinational companies had lawyers and consultants engaged in expensive and distracting internal investigations around the globe. The DOJ has proclaimed that the rationale for aggressive enforcement is its mission to protect consumers. In its 2013 Resource Guide to the U.S. FCPA, the DOJ states: "[c]orruption has corrosive effects on democratic institutions, undermining public accountability and diverting public resources from important priorities such as health, education, and infrastructure. When business is won or lost based on how much a company is willing to pay in bribes rather than on the quality of its products and services, law-abiding companies are placed at a competitive disadvantage — and consumers lose."

The key FCPA sections provide for criminal prosecution for the bribery of foreign government officials and, for those companies that issue securities subject to the jurisdiction of the SEC ("issuers"), for inaccurate record-keeping and inadequate internal accounting controls. While individual prosecutions have been infrequent, the DOJ is always publicizing its intent to increase arrests and prosecutions. In 2010 Congressional testimony, the DOJ took the position that "the department has made the prosecution of individuals a critical part of its FCPA enforcement strategy" because it is considered "an important and effective deterrent." The DOJ makes similar proclamations annually, but still retains a limited staff of prosecutors.

The anti-bribery provisions make it unlawful to "corruptly" offer or pay "anything of value" to a "foreign official" to assist "in obtaining or retaining business." These broad terms cover payments intended to influence a foreign official's decision-making or to help to secure a business advantage. The term "corruptly" has been interpreted broadly to mean that the offer or payment must have been "intended to induce the recipient to misuse his official position." Further, it is not necessary that the benefit be in the form of government business. For example, a payment that secures a business advantage, like favorable tax treatment or reduced customs duties, is prohibited. Courts have defined "anything of value" to include both tangible and intangible benefits. For example, promises of future employment and even sex have been

found to constitute value. *United States v. Gorman*, 807 F.2d 1299 (6th Cir. 1986) and *United States v. Moore*, 525 F.3d 1033 (11th Cir. 2008).

U.S. Enforcement

FCPA enforcement is different than most federal criminal laws. First, the FCPA is enforced by the Fraud Section (FRD) of the DOJ Criminal Division in Washington, DC. At its discretion, the FRD may delegate authority to any U.S. Attorney's Office to join an investigation and prosecution. Otherwise, it is a limited group of prosecutors at main justice handling the cases.

Of the nine areas the DOJ claims to evaluate when deciding whether to bring a criminal case against a business, it has focused on the effectiveness of compliance programs as a key surrogate in its decision making process. The nine stated areas include: 1) seriousness of the crime; 2) pervasiveness of wrongdoing within the business; 3) history of similar misconduct; 4) voluntary disclosure; 5) existence and effectiveness of a compliance program; 6) remedial actions; 7) collateral consequences; 8) adequacy of individual prosecutions; and 9) adequacy of other remedies. The DOJ has recognized that "no compliance program can ever prevent all criminal activity" by employees, but it nevertheless intends to focus on compliance program "design and good faith implementation and enforcement" and whether the program promotes a "culture that encourages ethical conduct and a commitment to compliance with the law."

Formal Programs

After the Federal Sentencing Guidelines laid out the benefits of having a compliance program, many well-intentioned companies adopted formalistic programs. However, certain "check-the-box" compliance programs were ineffective, inefficient, and drove a wedge between operations and the compliance personnel. Many of these initial programs were not designed to address a specific business's practices, needs, risks, and challenges. Further, the programs were not able to adjust with acquisitions, product launches, regulatory transformation, or global political changes. Thus, over time some compliance programs have become frustrating for operations and viewed as restraining productivity.

The problems with these initial compliance programs were numerous. When independent compliance departments were created, they were too far removed from the business functions and management. This led to a perception at some companies that the compliance personnel were policing business in an adversarial manner. Further, managers tended to see business functions as their responsibility, and compliance as the responsibility of the compliance department. Training implemented by compliance personnel tended to be formalistic and removed from real world, industry specific examples because it was not designed by operations. With increasing expectations from governments worldwide that companies manage risk effectively, moving to embedded processes and structures that focus on the value of business integrity can improve compliance and avoid some of the problems with older model programs.

Business Integrity Plans

In its guidance, the DOJ asserts that corruption is anti-competitive, increases the cost of doing business, inflates the cost of government contracts in developing countries, and introduces uncertainty into business transactions. In addition, directors and managers understand that corruption is bad for business and that an ethical culture with the appropriate "tone at the top" is important. One message that may have been forgotten is that companies can directly market integrity to gain an advantage. As counsel, expressly advocating for comprehensive embedded processes can reduce potential risk and exposure, and it can be a component of improving company stature and image. In turn, if company counsel should ever need to directly address the DOJ, it should be prepared to address governmental concerns at a level that should discourage intervention. Companies also need to consider that corruption is bad internally because it can undermine confidence in management and can cultivate employee self-dealing.

In 2011, the National Business Ethics Survey singled out "[e]thical culture" as "the single biggest factor determining the amount of misconduct that will take place in a business." Such a finding, however, is not much help to businesses that want to take affirmative steps to improve compliance. Embedding compliance means establishing incentives, penalties, and transparent processes that reward and punish employees on integrity based issues.

Companies can start by integrating compliance programs into business functions and decision-making. Encourage the following steps: appoint and rotate compliance officers from within business units; require managers to incorporate compliance in daily decision-making; increase individual accountability; place compliance-related requirements in performance plans; and staff compliance committees with individuals from varied business units.

In addition, companies should enact concise, communicated, accessible, and attainable codes of conduct. The code needs to be applied uniformly to all employees. The code and all compliance procedures should be developed based on the company's business model, including its products and services, third-party agents, customers, government interactions, and industry and geographic risks. Not all businesses face the same risks, so it is wise to consult with counsel who understands your business sector, as well as the enforcement and regulatory environment. Companies should do risk assessments within divisions and business units to identify areas that present high-risk transactions and geographic locations and allocate resources accordingly, with a focus on high-risk transactions and locations.

The DOJ explained that "[d]evoting a disproportionate amount of time policing modest entertainment and gift-giving instead of focusing on large government bids, questionable payments to third-party consultants, or excessive discounts to resellers and distributors may indicate that a company's compliance program is ineffective." Also, "performing identical due diligence on all third-party agents, irrespective of risk factors, is often counter-productive" as it diverts resources and attention away from high-risk areas. Simply put, companies should be less concerned with technical compliance and legal ambiguities, and more concerned with

reflecting good business judgment, proper intentions, and a desire to do business with integrity.

Management must invest in the process to embed principles and practices into their daily lives. After educating management on existing laws, the regulatory landscape, and enforcement trends, have the business units in key areas compile lists of high risk activities and warning signs. After evaluation, focus integrity training programs around these lists and update the process based on new discoveries. Employee training should be based on key principles (e.g. , financial integrity, record keeping, sound business judgment, and promoting integrity to gain business advantage) with industry specific examples. Ask management how to design processes that eliminate frustration with compliance bureaucracy and try to develop ownership in values-based decision-making.

When an issue arises, companies need to fully and expeditiously investigate. If integrity violations occurred, those responsible should be disciplined and the responsible business unit needs to address the risk by identifying the root cause and any systemic weaknesses.

Conclusion

The primary goal of compliance should be establishing and fostering a compliance culture. Only secondarily should companies consider how effective plans can serve to assist in the event of a government investigation. The idea of proving up the effectiveness of compliance programs in the face of an investigation may seem counterintuitive. However, companies that are prepared can substantially reduce expense and overall risk by establishing the effectiveness of embedded compliance programs.

Kirk Ogrosky and **Jeffrey Hessekiel** are members of the White Collar Criminal Defense and FDA/Healthcare Practice Groups at Arnold & Porter LLP. Prior to joining the firm, Mr. Ogrosky was the head of healthcare fraud enforcement in the Criminal Division of the U.S. Department of Justice from 2006 to 2010, and Mr. Hessekiel was the Chief Compliance Officer of Gilead Sciences Inc. from 2007 to 2012.