



**Complying with the
Foreign Corrupt Practices Act
(FCPA)**

Complying with the Foreign Corrupt Practices Act (FCPA)

The Role of Continuous Monitoring in an Effective Compliance Program

The Foreign Corrupt Practices Act (FCPA) was passed into law in 1977. The FCPA can be broken down into two parts, violating either of which constitutes a separate offense. The first part addresses anti-bribery. In this area, the FCPA is an extension of previous anti-bribery provisions that have been applied to US companies and US citizens for a long time. The second element of the act addresses accounting requirements—the things that an organization has to do in order to maintain records that accurately reflect transactions and the nature and quantity of corporate assets and liabilities. Ultimately, under the FCPA it is illegal to make payments directly or indirectly to foreign officials, officials of foreign political parties, or any other person who is acting as a conduit for payments to foreign officials or political parties, with a corrupt motive—that is, with the express purpose of influencing that official in order to obtain or retain business.

The Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) have significantly stepped up enforcement of the FCPA – and promise more to come.

The Field of Enforcement

The FCPA applies to US nationals and residents and US companies, as well as companies that are listed on US stock exchanges, and prohibits this kind of influence peddling whether or not it is an “accepted” practice in a local circumstance. With stepped up enforcement, complying with the FCPA has become increasingly a topic of conversation and concern not only among US companies, but also among those that operate outside of the US, but fall under FCPA provisions.

Two different organizations are involved from an enforcement perspective: The Department of Justice (DOJ) on the criminal enforcement side, and the Securities and Exchange Commission (SEC) on the civil enforcement side. For the DOJ, FCPA enforcement is about fraud in the context of anti-bribery. SEC enforcement is from the perspective of the impact of FCPA violations on the value of businesses—ensuring that those values are not inflated as a result of illegal activities. Both organizations have significantly stepped up enforcement activities over the past two years. For example, the SEC reports that since January 2006 it has brought 38 FCPA enforcement actions - more than were brought in all prior years combined since the FCPA became law in 1977.

The DOJ has similarly stepped up their FCPA enforcement efforts. At a C5 anti-corruption conference in Frankfurt on January 27th, the DOJ representative is reported to have made the following enforcement trend predictions for 2009:

- The level of enforcement is at an all-time high and is likely to remain there.
- Prosecuting senior company executives in their individual capacities will be a priority.
- The US will investigate US and foreign issuers equally, as well as companies operating within US territory.
- The DOJ and FBI are committing more resources to FCPA enforcement.
- FCPA due diligence will be a regular feature of mergers and acquisitions and transactional work.

- Increased enforcement of other crimes, alongside FCPA violations, is expected, including money-laundering, export controls violations and false accounting.¹

The Consequences of Non-compliance

Individual prison sentences in particular have raised executive awareness and concern as to the impact of FCPA violations.

From a financial perspective, non-compliance with the FCPA can have significant consequences. On the criminal side, companies can be fined \$2 million per violation of the anti-bribery provisions, and individuals can be fined up to \$250 thousand per violation, as well as being subject to up to five years in prison. Each intentional violation of the books-and-records and internal control provisions can result in a \$25 million fine for a company, and up to \$5 million and 20 years in prison for culpable individuals. The prison consequences in particular—especially in light of the DOJ’s stated priority of prosecuting senior executives—have raised executive awareness and concern as to the impact of FCPA violations. There are also consequences from a civil perspective, such as termination of government licenses and debarment from government contracting programs. In addition, the SEC can require disgorgement of a company’s profits on any contracts that are judged to have resulted from improper payments.

There is a third category of significant costs when it comes to addressing an FCPA investigation, whether it is opened by the DOJ or the SEC. These are the costs that arise from the requirement for the organization to produce documents that could be related to an FCPA violation. Typically, there are third parties – law firms and consulting firms that specialize in FCPA – involved in producing the documents required by the DOJ or the SEC. Charges for these third-party services range in the high hundreds of dollars per hour. This can drive the cost of gathering the required documentation into the tens of millions of dollars.

Anti-fraud Climate Drives FCPA Increase

The question often comes up, “Why FCPA? And why now?” The FCPA has been around for more than thirty years. Why the recent increase in interest in FCPA enforcement on the part of the DOJ and the SEC? The number of actions prior to two years ago was in the dozens, and suddenly in the course of a single year there have been up to 30 actions brought by the DOJ.

According to Shearman & Sterling LLP’s “FCPA Digest” of March 2009, the increase in FCPA prosecutions over the past several years can be attributed to an increase in voluntary reporting by corporations (possibly due to government emphasis on rewarding cooperation and disclosure, as evidenced by the growing willingness of the DOJ to enter into deferred or non-prosecution agreements in such cases); and to increased international law enforcement cooperation, which facilitates investigation and prosecution; as well as to a renewed focus on internal

In today’s global economy, with a real distaste for fraud and bribery, the DOJ and the SEC think of anti-bribery as being a ‘white-hat’ sort of action that they can bring.

¹ Wrage, Alexandra A. "FCPA Enforcement: Top Ten Trends for 2009." [wrageblog Anti-Bribery Compliance blog](http://wrageblog.org/2009/01/28/fcpa-enforcement-top-ten-trends-for-2009/). 28 Jan 2009. 11 Mar 2009 <<http://wrageblog.org/2009/01/28/fcpa-enforcement-top-ten-trends-for-2009/>>

controls and the Sarbanes-Oxley (SOX) requirement of executive certifications.²

But fundamentally, the increase really comes down to the anti-fraud climate that exists today in the US and, increasingly, throughout the world. Whether you call it the “post-Enron”, or “post-WorldCom”, or even, in current terms, the “post-Satyam” environment, there is a real distaste for fraud in general and bribery in particular. In this climate, the DOJ and the SEC think of anti-bribery as being a ‘white-hat’ sort of action that they can bring. As opposed to going after a company for a SOX violation, which seems like something that is punishing US businesses, going after someone who is bribing foreign officials brings into account two very bad things: One, bribery, and the other one, foreign. For the DOJ in particular, the FCPA serves as the business equivalent of the RICO act—a way to go after businesses that might be doing things that are distasteful in other contexts.

Pushing for Proactive Controls

One of the DOJ’s key concerns is that too many companies lack proactive FCPA controls and compliance procedures. The concern at the DOJ with the insufficiency of early disclosure, and a real desire for companies to do more in order to protect against FCPA violations, is borne out in the types of agreements that are reached when companies come to an agreement with the DOJ after an investigation has been completed. The DOJ has been much more tolerant of organizations which have been more proactive and can outline programs that are in place than they have been with companies that have been less so. Unfortunately, many companies have failed to take advantage of this opportunity to mitigate the potential impact of an investigation.

This could be seen, for example, at an industry conference in 2008, where certain chief compliance officers detailed how their companies are doing leading-edge data mining in order to proactively address FCPA compliance. In question and answer sessions in these presentations, the majority of inquiries were not about this proactive approach. Instead, the questions reflected a doggedly old-school approach – what hotline they were using, the hours of operation, the languages in which the hotlines were being answered – with relatively few questions asked about the ingenious leading-edge data analytics the presenting organizations were using to address potential FCPA violations.

The discussions at this conference reflect a general tendency to sit back and expect fraud to reveal itself through a hotline, a tip, or a whistle-blower. This in spite of the fact that experience shows these tools to be less effective anti-fraud controls than proactive data mining, or the use of electronic footprints within an organization to gain a greater understanding of what might be going on. The DOJ’s interest in companies being more proactive is much more likely to be satisfied through the latter approaches than through a company increasing the availability or number of languages used to answer hotlines.

² "Recent Trends and Patterns in FCPA Enforcement." [Shearman & Sterling LLP](http://www.shearman.com/files/upload/LT-030509-FCPA-Digest-Recent-Trends-and-Patterns-in-FCPA-Enforcement.pdf). Mar 2009. Shearman & Sterling LLP. 13 Mar 2009 <<http://www.shearman.com/files/upload/LT-030509-FCPA-Digest-Recent-Trends-and-Patterns-in-FCPA-Enforcement.pdf>>.

Transparency International's Corruption Perception Index

Founded in 1993, Transparency International (TI) is a global network of locally established national chapters that fight corruption on the ground, as well as through global and regional initiatives.

Politically non-partisan, TI developed the Corruption Perception Index (CPI) to rank countries in terms of the degree to which corruption is perceived to exist among public officials and politicians.

The CPI reflects views from around the world, including those of experts who are living in the countries evaluated.

SOURCE: <http://www.transparency.org/>

The Nature of FCPA Violations

In order to create a proactive compliance program, it is important to understand exactly what can happen to constitute an FCPA violation, to recognize common schemes and learn how violations occur. Keep in mind that for businesses in the US doing business outside of the US—any business, anywhere—there is a potential for FCPA violations to occur. This potential escalates as the business is conducted in countries—in particular many in South America, Africa, the Middle East and Asia—with a higher Corruption Perception Index (CPI). *See sidebar.*

Common bribery schemes begin with nebulous fees, such as “finder’s” fees, occurring in countries with a high CPI. These are often recorded as consulting fees or referral fees, or as commissions, but they have the net effect of masking the fact that bribery has occurred. In essence, it is “laundering” the illegal exchange of monies by calling it something else.

A second, more direct, type of scheme involves the use of what we will call “perks”. For example, offering

training in a desirable destination location, such as Hawaii or Bali, rather than at the locally available facility. Perks could also refer to gifts that are not detailed, such as the use of automobiles or other vehicles, shopping trips, gambling junkets, club memberships, where the perks end up recorded as training, generic entertainment, or just direct cost. These sorts of unrecorded gifts are the kinds of perks that can constitute a violation of FCPA.

Another common scheme involves payments to advisors. These might be recorded as payments to consultants, or as “goodwill payments”, or they may be embedded in fees as additional billable hours. In many cases, ghost accounting, legal or consulting firms are used as the vehicle for this kind of bribery.

A more complex sort of bribery involves extending improper discounts on otherwise legitimate deals, or paying improper performance bonuses, or other such items that effectively constitute kickbacks. An example of this type of infraction is selling to a foreign official an item at the lowest price, when it is in fact an item that should be purchased at the highest cost. For instance, selling a vehicle to a government official at the cost of a stripped-down model of that vehicle, but delivering a vehicle which includes all of the expensive add-on options—navigation system, tricked-out wheels, all-leather interior, and so forth. In this case, the difference between the price which is being paid—the cost of the stripped-down model—and the real cost of the loaded model that is actually delivered ends up constituting the bribe itself.

Continuous monitoring can function as both a preventive and a detective anti-bribery control in a proactive FCPA compliance program.

The Role of Continuous Monitoring in a Proactive Program

There is a clear relationship between anti-bribery provisions and anti-fraud control because there is a very similar sort of relationship between the way that bribery is conducted and the kinds of schemes that are used for fraud. Take, for example, a fraud scheme that involves a slush fund. The associated fraud risks—misappropriation of

assets and falsified financial reporting—can be uncovered through continuous monitoring of financial transactions. In the same way, continuous monitoring can function as both a preventive and a detective anti-bribery control in a proactive FCPA compliance program.

A specific FCPA example might be an employee or agent who is providing payments to non-agent third-parties that are inappropriately benefiting a foreign official or related third-party. This constitutes an expenditure or liability that has been incurred for an illegal or improper use—a direct FCPA violation risk to the organization. Yet this is fundamentally the same kind of thing that occurs on an everyday basis within organizations, involving misuse and abuse of corporate assets and corporate processes. From a continuous monitoring perspective, there are all sorts of techniques that can be used to detect and ultimately prevent the improper use of corporate assets, and these apply equally for FCPA detection and prevention as for any other kind of misuse or waste in traditional business processes.

In looking at how continuous monitoring can be effectively used to combat the possibility of an FCPA violation, let's take the case of delivering nebulous fees to a foreign official as an act of bribery. There are a number of things that companies are doing today to try to combat those nebulous fees. One organization, for instance, has implemented a policy that no vendor which is described as an advisor, lobbyist or consultant, and which is located in a country with a high CPI figure, can be added to the company's master vendor file unless it is approved by the chief compliance officer of that organization. Since the policy was implemented, there have been no requests for new vendors described as a consultant, lobbyist or advisor. The question is, does that mean that there have been no lobbyists, consultants or advisors added to the vendor master file? Or there have been, but the policy was circumvented by entering such vendors under other descriptions. So how could continuous monitoring better serve the intended purpose of the policy, ensuring delivery of the desired *operational effect*?

Continuous monitoring can be used to automatically monitor and review every new vendor located in a high CPI country as each is added to the master vendor file, inspecting each to look for unusual characteristics, such as elements of the vendor record that are missing. In this case, the vendor record would be flagged as an "invalid vendor", a designation which kicks off an investigation to ensure that the suspect vendor is legitimate. Automated monitoring can further be used to inspect the transactions that are occurring with a particular vendor, once it has been flagged as higher risk. Red flags indicative of possible FCPA violations could include such conditions as being a one-time vendor, or the fact that payments to the suspect vendor are higher than they are for other vendors in the same category. In effect, monitoring can be used in order to keep an eye on a new vendor that might be considered suspicious, and to actually use the transactions flowing to that vendor as evidence in a more proactive investigation.

Continuous monitoring broadens the corporate view on FCPA compliance from sampling and hotlines to a risk view that is more universal and proactive in nature.

A second example of bribery described above involves the delivering of monies through entertainment, or through goods and services that have value, that end up as perks. Monitoring can enable companies to become more proactive in terms of understanding when that has occurred. Let's take the example of a high-risk country, where one of the executives has received a bonus that is completely out of the norm, either for a person in that position, for a person in that country, or for a person in an outside-of-the-US role. In order to identify such an unusual payment and determine whether it is legitimate, an organization might audit the activities of that individual on an ad-hoc basis—if the anomalous payment happened to come up in the normal

course of analyzing or auditing different areas of the organization. Continuous monitoring *ensures* that the inappropriate bonus is caught and investigated, by enabling the organization to effectively monitor all payments to

all executives at a certain level, and all payments to all employees within a certain market. In this way, it becomes very clear where payments are made that are out of the norm for a role, for a subsidiary, or for any other slice of the analysis. Monitoring executive payment alone might not tell you the whole story about potential exposure, but monitoring payment along with and in context of activities within the travel and entertainment budget as well as customer-related activities, makes it possible to see where T&E expenses, bonus payments and customer activities combined hold the potential for an FCPA violation.

Automated continuous monitoring takes an organization from having to rely on employees doing exceptional sorts of things in order to maintain a system, to managing by exception, proactively targeting and addressing situations that hold identified risk for the organization. Further, monitoring broadens the corporate view on FCPA compliance from the limited visibility inherent in sampling, or the isolated report that may come through on a hotline, to a risk view that is more universal in nature, enabling companies to be more proactive in addressing potential violations of the FCPA.

No News is Good News

In view of the financial challenges companies face in today's economy, many are wondering whether this is something that really needs attention and resources right now. They are asking, "How real is this for my organization? Could it happen to me? Why should I be concerned about this now?" The answer is, look at the daily news headlines. More and more companies find themselves getting news coverage that is a PR disaster, hammering investor confidence and driving profits—and stock prices—into the ground. For example, Michael Berman reports in the ABA Litigation News that Siemens AG pled guilty to charges of violating the FCPA and ended up paying \$800 million in DOJ and SEC penalties. And that was a financial "victory"—by leveraging its "extraordinary cooperation" (after the fact) Siemens was able to reduce a U.S. fine that had an upward range of \$2.7 billion. Similarly, Kellogg Brown & Root LLC (KBR), a former Halliburton subsidiary, agreed to a \$559 million settlement of bribery allegations involving Nigerian officials, and the company's former CEO, Albert "Jack" Stanley will be sentenced for his conspiracy in May.³ According to Danforth Newcomb, the founder of Shearman & Sterling LLP's FCPA practice, "Concern over FCPA matters may have been restricted to the internal compliance area in the recent past, but today FCPA and anti-corruption concerns permeate the organization—all the way to the CEO suite and the board of directors. No one wants to be the focus of a high-profile FCPA investigation or enforcement."⁴

The DOJ and the SEC are going to be much more lenient on organizations who've taken proactive steps to detect and report upon potential violations of the FCPA.

The list of companies being prosecuted for FCPS violations is out there, it's public, and it's growing. And it can't be too strongly emphasized that the costs of FCPA violations are not limited to the costs of defense, the costs of the fines, or the costs of any potential prison sentences. Significant costs are also incurred in terms of disruption to the organization, impact on reputation, and the resources required to produce the documentation required to effectively defend or negotiate the terms of a settlement with either the DOJ or the SEC.

³ Berman, Michael D.. "Siemens Rethinks Bribery as a Business Strategy." ABA Litigation News. 26 Feb 2009. American Bar Association. 16 Mar 2009 <<http://www.abanet.org/>>.

⁴ Newcomb, Danforth and Philip Urofsky. "Shearman & Sterling Publishes 2009 Foreign Corrupt Practices Act (FCPA) Trends and Patterns Report and FCPA Digest." Shearman & Sterling LLP News 09 Mar 2009 16 Mar 2009.

The impact—even the fact—of an FCPA investigation can be significantly mitigated through the use of automated monitoring systems in order to be proactive, to detect and prevent violations, and to facilitate necessary self-reporting. The DOJ and the SEC are going to be much more lenient on organizations who have taken proactive steps to detect and report upon potential violations of the FCPA than they are organizations who have not. Continuous monitoring constitutes that kind of proactive approach, and provides for the use of the leading-edge data mining approaches mentioned above to combat FCPA violations. Those organizations who are using these tools will be the companies that others will be compared against when the DOJ and the SEC come calling.

For more information about how global leaders use continuous monitoring to combat fraud and misuse, protect shareholder value and implement proactive compliance programs, visit www.oversightsystems.com.