Avoid an Investigation: Automate FCPA Compliance

BY SONNY CARPENTER

Consider a chief executive officer (CEO) or a chief financial officer (CFO) of a major multinational corporation working in the headquarters office at a large US city. Unbeknownst to either of them, one of their sales representatives 6,000 miles away in Kazakhstan is handing an envelope full of cash or a brand new tablet computer to a local government official in order to generate business for the corporation, violating the Foreign Corrupt Practices Act (FCPA). Who is liable? Is it the employee giving the bribe or the CEO/CFO 6,000 miles away? Because the government has the ability to impose "control person" liability, it is less than perfectly clear whether liability will stop with the sales rep or if it will reach the C-level executives. Because of this uncertainty, corporate officers can no longer remain in the dark.

Now more than ever, the regulators are enforcing compliance through automated software and creative legal means. The Securities and Exchange Commission (SEC) applies control person liability as a mechanism to hold corporate executives, board members, and companies liable for violations. One of the ways the government automates investigation of potential violations is by using the SEC's accounting quality model, or "RoboCop," to sift through corporate filings quickly. With technological advances in screening for risk and government enforcement tools such as control person liability, how is it possible for executives in the C-suite to ensure compliance with the law and internal controls? The solution lies in technology and automation. Corporations now must uncover inappropriate conduct faster and more efficiently to prevent intrusive government investigations.

Control Person Liability

Recent cases have confirmed that in its FCPA actions, the government has been targeting boards of directors, their members, and other corporate officers. (*See* SEC v. Nature's Sunshine Prods., Inc., No. 02-09 Civ. 0672 (D. Utah July 31, 2009) (naming the company's COO and CFO as defendants for the corrupt actions of the company and its employees under the defendants' supervision).) Section 20(a) of the Securities Exchange Act of 1934 (Exchange Act) places "control persons," such as the CFO or COO, in the crosshairs of a government investigation for corporate misconduct about which they should have known. Actions by other employees, such as bribing foreign officials, can be imputed to the control person, making that individual liable, so long as he or she should have known of the infraction. In *Nature's Sunshine*, the SEC charged that the COO and CFO were control persons responsible for the illegal acts of their subordinates, whom they did not properly supervise. (*Id.*)

Although not a new section under the Exchange Act, the SEC's use of § 20(a) to vigorously enforce the FCPA is a new way to ensure that corporate officers do not hide behind the veil of ignorance. More than ever, these control persons must keep an eye out for the FCPA "red flags" and be able to act quickly to ameliorate possible problems. Understandably, a robust compliance program must be implemented in a manner that not only protects the corporation but also provides the control persons with the ability to address potential FCPA problems. To protect themselves and to prevent violations, large businesses and their control persons are increasingly seeing the need to use technology and automation to ensure consistency of compliance monitoring across various divisions and offices.

Compliance Enhanced by Technology

The FCPA, which prohibits businesses from participating in corrupt activities, has three main components: prohibiting bribery of foreign officials, requiring maintenance of accurate books and records, and requiring implementation of internal controls. It is highly enforced, with the Department of Justice (DOJ) and the SEC leading the charge against corruption and bribery. A 2012 collaborative FCPA guide published by the DOJ and the SEC explicitly demonstrates the high priority the government places on FCPA enforcement. (DOJ Criminal Div. & SEC Enforcement Div., FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012), *available at* http://www.justice.gov/criminal/fraud/fcpa/guide.pdf.) A combination of increased oversight, these new guidelines, advances in technology, and an increasingly global marketplace have come together to make FCPA compliance a primary focus of the government and, consequently, corporate officials. As such, the compliance programs of corporations must be as robust as the government's enforcement efforts.

For example, take the case of a large *private* multinational company newly acquired by a *public* corporation. The acquiring company needs to determine quickly and efficiently any potential FCPA issues with the target company. Relying on internal spreadsheets,

SONNY CARPENTER *is an associate with BakerHostetler in the firm's New York office, where he practices in the area of complex commercial litigation.*

accounting records both computerized and manual, and outdated due diligence on outside business partners is not enough to ensure that a company is fully compliant with the requirements of the law. The DOJ and SEC guide offers "hallmarks of effective compliance programs" whereby efficiency and a wide-reaching culture of compliance are key components of these measures. (*Id.* at 57–62.) Commencing an internal investigation to find holes in the newly acquired company's compliance procedures is the first step in protecting oneself from the government. However, in these days of big data, immediate global communications, and instantaneous financial transactions, the corporation and its officers must incorporate new technologies into their compliance regimen to continually cull through the data to find threats that could become FCPA or other corruption concerns.

A technology platform can enable companies to monitor automatically various FCPA compliance areas such as training, accounts payable/receivable, purchasing, and third-party due diligence, thus, minimizing human error. A poll taken of attendees at a 2012 FCPA conference in Washington, D.C., revealed that the majority have no system to monitor high-risk third parties. (Marie-Charlotte Patterson, *Technology for minding your compliance P's and Q's: Spotlight on the FCPA*, Inside Couns. (May 2, 2013), http://tinyurl.com/nkdthwc.) Others indicated that they have no technology in place to help monitor, manage, and report on FCPA risks. (*Id.*) The sheer amount of information generated at large corporations demands a technical solution; otherwise there is a greater chance that the current internal controls will not catch FCPA risks. Large companies generate large amounts of data, and corporations need to have measures to constantly sift through the information to discover whether any corporate actions violate the law.

Some ways that technology solutions can assist in ensuring FCPA compliance include:

- Implementation of crawling software to continuously monitor key control areas to generate real-time information, cutting down on human error.
- Creation of red-flag analysis programs to monitor activity within traditionally suspect general ledger accounts such as travel, entertainment, political contributions, consultant fees, and petty cash. These analyses must include reviews of accounts in all corporate offices.
- Implementation of automated triggers to identify high-risk transactions such as duplicate payments, round-dollar amounts, cash distributions, and multiple payments to the same entity over a short time period.
- Adoption of a method to identify business conducted in or communications made to areas with a high corruption index or countries on the Office of Foreign Assets Control list.
- Automated monitoring of training programs to ensure completion and employee acknowledgment of FCPA guidance.
- The use of electronic audit trails to record access and changes.
- Electronic Sarbanes-Oxley monitoring to ensure the segregation of duties for various company personnel, including an alert system when the segregation is violated.

Conclusion

The reality of today's regulatory environment mandates that companies apply policies and procedures to reduce the risk of an FCPA violation. Applying technology to these FCPA compliance procedures is the best way to ensure that the company intelligently manages these procedures. Automating the enforcement of the company's policies as much as possible will reduce inconsistencies and missed data due to human error. Corporate executives, therefore, must have their current compliance procedures reviewed, determine the extent of the gaps in their compliance measures, and implement technological solutions before a government investigation reveals misconduct that should have been discovered earlier. These technological implementations will allow corporations to stay ahead of government investigators should they come knocking. In the event a violation occurs, the control persons can show the government that they and the company took appropriate precautions to detect FCPA violations. ■