A New Era of Cooperation and Compliance

How to navigate FCPA Investigations

By Carolyn Casey, J.D. / AccessData

The Department of Justice (DOJ) and Securities and Exchange Commission (SEC) continue to reveal insights on how to successfully navigate Foreign Corrupt Practices Act (FCPA) investigations. Recently, the government geared up to combat overseas bribery with the appointment of 10 new FCPA prosecutors – a 50 percent increase in dedicated FCPA attorney resources. In tandem, the FBI established three new squads of FBI agents to investigate and prosecute FCPA culprits. From DOJ implementation of the year-old "Yates Memo" to a slew of recent FCPA investigations, we are learning more about how corporations can cooperate to avoid negative outcomes.

Don't Hide Info on Individuals

Individual wrongdoers in FCPA or other corporate wrongdoing matters are having a harder time hiding among all the horses on the carousel. A year ago, the DOJ ushered in a new focus on holding individuals accountable for their fraudulent actions in corporate roles. "Americans should never believe, even incorrectly, that one's criminal activity will go unpunished simply because it was committed on behalf of a corporation," said Deputy Attorney General Sally Yates in a September 2015 speech. In what has become known as the Yates Memo, the deputy attorney general announced six new DOJ policies aimed at removing challenges to holding individuals liable for corporate wrongdoing. The new policies that continue to crop up in current investigations are:

1. No Individual Information, No Cooperation Benefits. To obtain any benefits from cooperating with the government, companies must give up the individuals involved, no matter their company rank. Further, companies that fail to continue to cooperate regarding prosecution of the individuals after securing any corporate plea and settlement agreements will be in material breach of those agreements.

2. No Delays on Individual Investigations. Government prosecutors will focus on the individual right from the start, regardless of whether the case starts civilly or criminally. This is intended to stop delays in individual cases during the corporate investigation, which can make later individual investigations more difficult.

3. Civil and Criminal DOJ Synergies. Department civil and criminal attorneys will cooperate a lot more during all stages of their investigations. The new policy contains specific directives on cross-unit communications and information sharing.

4. Approval for Exceptions to Common Start. Attorneys must write a justification for special circumstances and gain approval to proceed with any corporate investigations before the individual investigation commences.

5. Approval for Liability Releases. Government attorneys are only permitted to release individuals from civil or criminal liability when resolving a matter with a corporation under the rarest of circumstances. When such circumstances do arise, the litigating attorneys must obtain written approval from the relevant U.S. attorney or assistant attorney general.

6. Determining Factor Not Ability to Pay. The U.S. attorneys will pursue civil actions against corporate wrongdoers even if they lack the financial resources to satisfy a significant monetary judgment. In the past, decisions not to prosecute were sometimes made based solely on the inability to pay any eventual judgment.

Pilot FCPA Program

The Yates Memo was followed in the spring of 2016 by a new one-year FCPA Pilot Program.

"Bribery of foreign officials to gain or retain a business advantage poses a serious systemic criminal problem across the globe. It harms those who play by the rules, siphons money away from communities, and undermines the rule of law." Thus starts the DOJ Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance, which outlines the Pilot Program.

The Pilot Program, aimed at encouraging companies to voluntarily come forward with facts on questionable corporate and individual activities, offers some fairly specific guidance on how cooperation can result in benefits such as non-prosecution, faster resolution and lower fines. According to the Pilot Program, prompt and voluntary disclosure of relevant facts (including facts on individual misconduct), full investigative cooperation and timely remediation can lead to up to a 50 percent reduction in fines. In addition, under the program, if the company has implemented an effective compliance program, a monitor may not be assigned. Cooperation under the Pilot Program also increases the chances of avoiding full prosecution.

> ***Prompt and voluntary disclosure of relevant facts can lead to up to a 50 percent reduction in fines.***

Initial Pilot Program Cases

In June, the government announced the first two prosecutorial declinations under the Pilot Program. Both cases involved allegations that the company's Chinese subsidiary had engaged in bribery. Employees at Akamai's Chinese subsidiary provided $40,000 in improper gift cards, meals and entertainment to officials at state-owned entities to build business relationships. Nortek's Chinese subsidiary made improper payments and gifts to Chinese officials totaling $291,000 to influence regulatory actions and fines, according to the SEC.

Key Non-Prosecution Nortek Factors

Daniel Kahn, Director of the DOJ FCPA unit, outlined the key factors influencing the Nortek non-prosecution agreement.

- Company internal audit function identified the misconduct
- Prompt voluntary self-disclosure
- Thorough company investigation
- Full cooperation in this matter
- Identification of all individuals involved in or responsible for misconduct
- Provision to DOJ of all facts relating to the individual misconduct
- Agreement to continue to cooperate in any ongoing investigations of individuals
- Steps taken to enhance compliance program and internal accounting controls
- Full remediation
- Termination of all five individuals involved in the misconduct, including two high-level executives of the Chinese subsidiary
- Disgorgement of full amount to the SEC

Relatively Low Fine

In late August, after a 10-year investigation, AstraZeneca (AZ) agreed to pay $5.5 million to settle an FCPA investigation. Relative to an earlier $25 million settlement fee paid by Novartis, the AZ settlement seems like a walk in the park.

According to the SEC Cease and Desist Order, AZ's wholly owned subsidiaries in China and Russia failed to comply with FCPA internal controls and record-keeping requirements, allowing employees to generate cash using fake receipts, open bank accounts for doctors, and leverage a travel vendor to submit false expense invoices—all to make payments to influence healthcare providers' drug purchases and prescriptions. The government also alleged bribery of local Chinese officials to reduce or dismiss pending financial sanctions.

AZ Shows How to Cooperate

Even though AZ did not self-report, the SEC ruling cites AZ's subsequent voluntary and timely internal investigation disclosures, translations of key documents, and factual disclosures that would have proved difficult for the SEC to discover. The company's regular updates to SEC staff were also a positive factor. The key factors in the resolution were:

- Developed a centralized compliance program
- Revamped internal controls and procedures
- Enhanced its policies on gifts and entertainment as well as third-party engagements
- Added more training and audits
- Placed key compliance personnel in high-risk local markets
- Took several disciplinary actions involving employees, including demoting some, accepting voluntary separations and dismissing others

Carolyn Casey, J.D.
Senior Director, Industry Relations at AccessData. Carolyn analyzes market trends in digital investigations, e-discovery, compliance, global privacy and information governance.
ccasey@accessdata.com

No Prosecution of Cisco

In September, the DOJ and SEC declined to prosecute Cisco under the FCPA after Cisco fully cooperated, sharing their internal investigation of their Russian operations and resellers in nearby countries. Though public details are sparse, in what appears to be remediation steps, Cisco closed down its operation in Moscow that sold equipment to the Russian government, military and intelligence services. Eleven employees were either laid off or transferred, according to *Buzz News*.

Hedge and Private Equity Funds Not Immune

Finance ranks as the fourth most investigated industry under the FCPA over the last two years, according to the Shepard Mullin law firm. A high-profile FCPA investigation of the largest publicly traded hedge fund, Och-Ziff, signals that hedge funds and private equity firms should get their FCPA houses in order. Och-Ziff is accused of bribing Libyan officials to win business from the Libyan sovereign wealth fund, and of making illegal payments to the Democratic Republic of Congo. The New York–based company recently earmarked more than $400 million for a possible settlement with the U.S. government.

Takeaways

Here are few thoughts on what general counsels and chief compliance officers can take away from the last year of FCPA activity.

- Build the AZ and Nortek factors into your compliance programs and FCPA government investigations approach.
- Update your ability to audit and monitor the activities of employees, wholly owned subsidiaries and overseas partners with advanced forensics, "silent" searches and analysis tools.
- Double down on Chinese and Russian FCPA audits and monitoring.
- Be sure all employees in all locations get FCPA compliance training, especially sales reps.
- Reemphasize FCPA record-keeping and internal control requirements to accounting, HR, travel and managers.
- Consider placing compliance leaders in high-risk locations.
- Don't protect insiders; share findings on individuals with the DOJ and SEC to take advantage of the Pilot Program benefits.
- Take swift action to terminate bad actors.

INFORMATION GOVERNANCE INSIGHTS

By David White

Data Analytics May Hold Key to Compliance with South Korea Anti-Graft Scheme

New anti-graft laws that were promulgated by President Park Geun-hye on March 26, 2015 will take effect in South Korea this month.[1] Consistent with other efforts around the globe to combat corruption, the new legislation prohibits the transfer of value to any public servants, employees of public offices and state agencies, teachers, or journalists in excess of predefined amounts. For example, lunch or dinner shall be limited to a maximum of about $30, and gifts to $45. These can be doubled when they are given at family events such as weddings, funerals or the birth of a child. But if the value of the gift given exceeds these amounts, the offender shall be fined up to five times its value, and if it is more than about $850, criminal penalties shall be imposed.

Anti-bribery laws are not new in South Korea. In fact, South Korea was one of the first signatories at the OECD Anti-Bribery Convention in 1997, and in the following year it enacted legislation – the Act on Preventing Bribery of Foreign Public Officials in International Business Transactions (Korean FBPA) – to implement the convention domestically.[2] Criminal and civil penalties for domestic acts of bribery have also been on the books for many years, seeking to discourage both private and public transfers of value in return for favors. However, there are several key differences in the new anti-graft law that may require companies doing business in Korea to reevaluate their compliance programs.

Prior to the anti-graft law, penalties for domestic bribery were only levied after confirming a connection between the received gifts or favors and the activities of civil servants. Under the new law, it is no longer necessary to prove any purpose behind the gift. The gift itself is enough to establish culpability. More importantly, the preexisting anti-bribery laws did not typically impose liability on corporations for bribes made by its employees. Under the new anti-graft law, corporate criminal liability may be imposed for violations by employees, unless the corporation can show it exerted due care and supervision to prevent such a transfer. This latter change will likely entice companies doing business in Korea to ramp up their supervision and compliance controls. But what level of supervision and controls do these companies really need?

Modern technology can greatly assist in assessing what anti-corruption controls are most appropriate.

Experience from other jurisdictions dictates that the optimal type, placement and quantity of controls is largely driven by the context in which a company operates, the level of the government officials with which a company interacts, and the types of relationships or interactions a company has with those government officials. To assess the risk inherent in a given activity, a company should work to identify and quantify potential transfers of value to regulated recipients. Gifts, travel, meals, jobs for relatives and even contributions to charities may be considered value that could influence the decision-making of the government official, teacher or journalist. All of these factors determine where and by whom the review or approval should be conducted. It is also important to review these activities and provide a mechanism that allows consistent application of this prereview process throughout the organization, with appropriate record keeping and oversight. Companies can't simply ask people to self-report their expenses and then raise flags when value transfers exceed the statutory limits. Doing so would simply convert overt graft giving to covert money laundering schemes where transfers become hidden.[3]

Fortunately, modern technology can greatly assist in these efforts. One of the most efficient ways that companies can assess what anti-corruption controls are most appropriate is by gathering historic expense and communications data and analyzing specific activities. Predictive analytics tools can then be leveraged to map existing relationships with public officials based on past behavior, and machine-learning algorithms can be used to identify potential future risks related to gift giving. Companies can leverage such tools to properly match the intensity of their controls with the identified risks for each particular activity. Basing assessments on actual data ensures that organizations are deploying their resources both in the right areas and in ways that maintain the defensibility and credibility of the compliance process. Compliance programs will not be supported if they are viewed as an impediment to conducting efficient business and appear unnecessary given perceived risk. This in turn makes it much more difficult to maintain the exact mechanisms that mitigate critical risk, which are expected by government regulators. Since the essence of a compliance program is the prevention, detection and remediation of wrongdoing, a company's resources should be allocated to activities that pose the highest risk – and with proper data analytics these risks can easily and efficiently be identified and addressed.

To review the footnotes to this article, visit http://www.metrocorpcounsel.com

AlixPartners

David White is a director at AlixPartners LLP, where he advises clients on information governance, information security and electronic discovery. He can be reached at dwhite@alixpartners.com.