The FCPA REPORT

www.fcpareport.com Volume 5, Number 18 September 14, 2016

Five Ways a Company Can Leverage Its Anti-Bribery Compliance Program to Facilitate Sanctions Compliance

By Ryan Fayhee, Geoff Martin and Alexandre Lamy
Baker & McKenzie

While often treated separately by companies, anti-bribery and sanctions compliance risks frequently intersect because they arise from a common exposure to extraterritorial jurisdiction as well as a common susceptibility to enforcement standards, often as a consequence of an overlapping focus on certain high-risk markets and similarly positioned employees and third parties.

In this article, we will first review how the jurisdictional reach and risks presented by anti-bribery and sanctions regulations tend to converge. We will then suggest concrete ways that companies can leverage their anti-bribery compliance programs to facilitate sanctions compliance. Companies can ensure effective compliance with both types of regulations more efficiently, effectively and economically by combining certain knowledge and resources to jointly address these areas.

See "Anti-Corruption and Trade Regulations: Identifying Common Elements and Streamlining Compliance Programs (Part One of Two)" (Jul. 9, 2014); and Part Two (Jul. 23, 2014).

Converging Compliance and Enforcement Risks

Extraterritorial Reach

The FCPA and U.S. trade sanctions regulations both have significant extraterritorial reach.

Although the FCPA technically applies only to (1) U.S. domestic concerns or issuers of securities, or any officer, director, employee, or agent thereof (regardless of their nationality); (2) any U.S. citizen, whether inside or outside of the U.S.; and (3) any other person, while in the territory of the U.S., prosecutors espouse a very broad view of jurisdiction under the statute.

Specifically, the DOJ and SEC have adopted a very expansive interpretation of when non-U.S. entities or persons are considered to be acting as "agents" of U.S. entities, persons or issuers, and what constitutes an act committed "in the territory of the U.S." to attract jurisdiction. The jurisdiction of the FCPA is further extended by the aggressive use of inchoate offences such as conspiracy and aiding and abetting to charge non-U.S. companies or individuals who participate in bribery schemes with others who are subject more directly to U.S. FCPA jurisdiction.

Similarly, U.S. sanctions programs generally apply to "U.S. Persons," a category that includes all U.S. citizens and permanent residents regardless of their location, all parties physically located in the United States, and all entities organized under U.S. laws and their non-U.S. branches. In the case of the U.S. sanctions targeting Cuba and Iran, the U.S. Government also claims jurisdiction over non-U.S. subsidiaries owned or controlled by U.S. Persons. In addition, U.S. laws and regulations impose prohibitions and restrictions on U.S. and non-U.S. parties exporting, reexporting, and transferring goods, software, or technology of U.S. origin or non-U.S. origin that incorporate more than de minimis levels of U.S. content, wherever such items are located and even after export from the United States.

Taken together, the similarities in the extraterritorial scope of these programs are such that actions taken abroad by U.S. persons and companies very often come within the jurisdiction of both legal regimes. For example, a local sales representative employed at a foreign subsidiary of a U.S. company who makes an improper payment to a Cuban government official in order to secure a contract for an order of goods would likely create liability for the U.S. parent company under both the FCPA and the Cuban Assets Control Regulations (CACR).

This situation is exacerbated when employees or management of non-U.S. subsidiaries are unfamiliar with the requirements of these U.S. regimes and unaware of how their activities might trigger U.S. jurisdiction and liability. Further complicating matters, in many cases, U.S. requirements will differ, and in

some cases actively conflict, with the requirements placed on the company under local law.

As the jurisdiction of both regimes is expansive, non-U.S. companies should carefully assess their activities implicating a U.S. nexus to evaluate their potential exposure to U.S. law, and ensure that all group companies are aware of the requirements and potential exposure. There are some differences, and complexities in the jurisdictional reach of each of these regimes, which must be considered separately. For example, a non-U.S. company that has securities that are publicly traded in the United States would be exposed to the jurisdiction of the FCPA but not to most U.S. sanctions programs absent some other nexus to the U.S.

Exposure in Similar Markets

Industries and markets with high risks of corruption also tend to have higher sanctions risks. The oil and gas, energy, mining, and defense industries present high risks in both contexts because they tend to involve interactions with government officials and politically strategic industries, and are therefore more likely to involve transactions with designated parties than other industries.

Certain countries and regions also present similarly convergent risks. For example, those countries subject to comprehensive sanctions, and in which designated persons are concentrated, tend to be countries which also face a significant corruption risk.

Exposure From Similarly Positioned Employees and Third Parties

The same employees tend to be at the highest risk of causing a company to commit both FCPA and sanctions violations. In particular, absent sufficient instruction and monitoring, customer-facing sales employees in high-risk jurisdictions may be tempted to cut corners or turn a blind eye to red flags in order to make a sale, meet their targets, or increase personal commissions or bonuses.

The accounting and finance team, either locally or at a company's head office, will also almost always be involved as well, either by entering or approving a relevant financial transaction in the company's systems, or by registering a third-party customer or vendor who ultimately causes the company to be in breach of anti-bribery rules or sanctions. Additionally, under both the FCPA and sanctions regimes, a company can be held liable for actions taken by third parties on its behalf. Indeed, bribes and sanctions violations are often not made by companies directly. Rather, illicit bribe payments are commonly paid through agents and intermediaries before finding their way into the ultimate beneficiary; likewise, sales to sanctioned countries and restricted parties are often made through convoluted supply chains before products find their way to their ultimate destination or customer. These structures are often deliberately established by company employees to obfuscate the true purpose of the transaction in question from the company's management, finance or compliance teams, or from local law enforcement. The recipients of bribes or products may be similarly motivated to conceal their own conduct by introducing intermediaries between them and the company.

Third parties with which a company does business are typically outside of a company's core systems and controls. This lack of visibility and control means that such third parties can be at a greater risk of paying bribes on a company's behalf and selling into sanctioned countries or to restricted parties.

Knowledge Standards

The knowledge requirements of the FCPA are complex, depending on which provision of the statute is being charged, whether the defendant is an individual or a corporation and whether the resolution is made via civil or criminal means. However, generally speaking, establishing an FCPA violation requires prosecutors to demonstrate that a person's state of mind be "knowing" with respect to the conduct, circumstances, or result in question. Such knowledge can be established through a showing of either actual awareness or belief, or through "willful blindness," which occurs when a person deliberately avoids actual knowledge or is ambivalent to the same. As with jurisdiction, U.S. authorities generally quite readily establish the requisite knowledge or willful blindness necessary for an FCPA violation.

Similarly, while offending parties are strictly liable for civil penalties for U.S. sanctions violations, such violations are more likely to be classified as egregious and penalized more severely (or referred for criminal prosecution) if there are indications that the responsible parties had actual knowledge

or "reason to know" of the violation. Under both regimes, the requisite constructive knowledge is often established due to a company's lax compliance and controls environment leading to its limited visibility of the parties with which it is doing business, and their activities.

Identification of Violations

The ways in which violations of the FCPA and sanctions regulations tend to come to light are also similar. Companies are often faced with whistleblower reports that may vaguely allege a breach of U.S. law, or enumerate circumstances that could constitute violations of either or both regimes. Whistleblowers in both spheres are being increasingly encouraged and incentivized to approach U.S. enforcement agencies directly with allegations of violations.

Finally, both regimes tend to present issues when companies are merging or acquiring other entities. Issues may come to light as part of the pre-acquisition due diligence process, or after acquisition when the two companies are being integrated.

Leveraging FCPA Compliance Programs to Make Sanctions Compliance Easier

Fortunately, while these intersections underscore the compliance challenges these legal regimes have in common, they are also suggestive of ways that companies can be proactive in leveraging these intersections to facilitate compliance. Accordingly, companies that address these risks using an integrated compliance program can significantly mitigate the potential for violations under both legal regimes.

1. Set a Strong Tone of Compliance from the Top of the Company

In both FCPA and sanctions compliance, a commitment to compliance must be set from the highest levels of the company. Local management (particularly in high-risk countries) can also help to ensure compliance by reiterating its importance to employees and stressing that a blind eye will not be turned to potential violations. This commitment to compliance must be clearly and regularly communicated to employees in all parts of the business, thereby establishing a strong culture of compliance throughout the organization, driven by the example of management.

See "How to Build a Compliant Culture and Stronger Company From the 'Middle' (Part One of Three) (Apr. 1, 2015); Part Two (Apr. 15, 2015); Part Three (Apr. 29, 2015).

2. Target High-Risk Employees

Effective compliance with both FCPA and sanctions rules requires that a company identify its risk profile and target its resources accordingly. As such, employees who are at the highest risk of both FCPA and sanctions violations, including sales employees located in high-risk areas, or who might sell into high-risk jurisdictions, should be the focus of both compliance training and monitoring for both subject matter areas.

The highest priority should be providing live, in-person training to country managers, directors, officers, sales employees, and third-party intermediaries who have direct contact with government officials or who deal with state-owned entities. During live training, employees are more likely to mention potentially risky practices, which may provide the company with an opportunity to remediate any problems before they lead to violations. Computer-based training may be appropriate in addition to live training, as a refresher and as a solution for lower-risk employees.

Similarly, finance and accounting employees should be trained and empowered to identify red flags with potentially high-risk transactions and to escalate them for review and further approval as necessary. The finance team is often the first line of defense against improper engagements, payments, or transactions being authorized.

In addition, training should extend beyond providing an overview of the FCPA and non-U.S. anti-bribery laws, sanctions regulations, and enforcement trends to include a discussion of specific risks faced by employees in the country and industry where they are working. For example, a training session conducted in Russia should address the kinds of transactions that mostly often implicate the FCPA and sanctions rules there, the mechanics of screening for the presence of restricted parties, the types of transactions that are prohibited for U.S. companies under U.S. sanctions, and the importance of staying abreast of an evolving legal situation.

3. Target Third Parties

As discussed above, third parties can be used or involved in bribery and sanctions violations schemes in a myriad of ways to disguise the true beneficiaries or destinations of a transaction. It is therefore essential to fully understand the universe of third parties with which the company does business and the risks that they present. This is likely to involve conducting risk-based due diligence during the on-boarding of third parties, the imposition of robust contractual protections, and the exercise of effective oversight and control during third-party engagements.
See "The Emperor Is Far Away: The Evolving Nature of Third-Party Risk in China" (Sep. 9, 2015).

Due Diligence

Appropriate due diligence will depend upon the risk profile of the third party being engaged and should include requiring third parties to complete background questionnaires detailing their financial stability, government ties, affiliations with restricted parties, and any history of investigations, enforcement or litigation. In addition, companies are often well advised to conduct background checks on partners in high-risk markets to ensure that they have represented themselves accurately and to identify any further red flags prior to engagement.

All third parties should be cross-checked against sanctions and restricted parties lists prior to their engagement. Many modern screening solutions allow this to be relatively automated within the customer on-boarding process.

Contractual Rights

Third parties should be required to warrant their commitment to compliance with relevant laws in their engagement contract and even annually in a signed certification form. A company should also empower itself with contractual rights to audit and monitor the conduct of third parties and negotiate for the right to terminate the contact if the company later determines that the third party has engaged in misconduct, unethical behaviour, or illegal activity.

See "When and How Should Companies Include Audit Rights in Third-Party Contracts? (Part One of Three)" (Jul. 23, 2014); Part Two (Aug. 6, 2014); and Part Three (Aug. 20, 2014).

Ongoing Monitoring and Mitigation

These risk assessment and mitigation measures during the on-boarding process may be insufficient to ensure compliance once the contract has been signed, unless the third party is actually and adequately monitored throughout the engagement. Regularly auditing relevant financial controls (e.g., around payments to third parties and supporting documents) can help to quickly identify and resolve any problems. In other circumstances, it may be appropriate to have certain high-risk third parties attend the company's own compliance training sessions.

4. Establish Strong Accounting Controls, Implement Continuous Monitoring and Auditing

Strong accounting controls can help to ensure that payments are not being made to parties that would create FCPA or sanctions compliance risks. The FCPA affirmatively requires issuers to book transactions correctly to accurately reflect the disposition of the company's assets.

Special attention should be paid to suspicious payments or withdrawals that could indicate off-the-books transactions and to transactions with consultants, business development agents, charitable and political contributions, and gifts and hospitality involving government officials. Internal audit protocols can be developed to specifically test and identify anomalies in these areas.

5. Respond Quickly and Effectively to Concerns Raised

Company internal reporting and investigation protocols can also be leveraged to quickly identify and respond to potential FCPA and sanctions issues alike. If employees are well informed and know where to go to ask questions or report concerns (such as through an ethics hotline), then they will be more likely to be comfortable bringing such concerns to the company's attention (whether they be related to FCPA or sanctions compliance).

In both areas, a company's response to a violation can significantly reduce or eliminate the resulting penalties that the company may face. Both regimes allow for companies to

make voluntary self disclosures of actual or potential violations and receive credit for doing so.

To ensure that it is empowered to quickly understand any potential issues and to utilize these mechanisms should a violation occur, a company should ensure that it has a well-resourced internal investigations function and a clear protocol on how to respond to allegations in each area. This function should be well informed of the various areas in which the company may face liability, including under the FCPA and sanctions regimes.

Ryan Fayhee is a partner in the Washington, DC, office of Baker & McKenzie LLP. Mr. Fayhee previously was with the U.S. Department of Justice for more than a decade, where he was a leading national security prosecutor in the areas of economic espionage, export controls, sanctions enforcement, and cybercrime.

Geoff Martin and Alexandre Lamy are senior associates in the same office of Baker & McKenzie. Mr. Martin's practice focuses on anti-corruption compliance and investigations, particularly under the FCPA and the U.K. Bribery Act. He is admitted to practice in both jurisdictions. Mr. Lamy's practice focuses on U.S. export controls and trade sanctions.

The authors are grateful for the assistance of Daniel Andreeff in the preparation of this article.