Anti-Corruption Report
An Acuris company

anti-corruption.com

June 24, 2020

THIRD PARTIES

Naming Bribe-Paying Third Parties Would Improve FCPA Compliance

By David Simon, Christopher Swift, Olivia S. Singelmann and Jenlain A. Scott, *Foley & Lardner*

The vast majority of modern FCPA enforcement actions have involved improper payments made not by company employees but by third-party intermediaries acting on the company's behalf. Notwithstanding the fact that third-party intermediary relationships pose the greatest risk of foreign bribery in violation of U.S. law, and the DOJ and the SEC's high compliance expectations, the DOJ and SEC generally do not disclose the names of bribe-paying third-party intermediary companies and individuals in their FCPA resolution documents. There are obvious and valid due process reasons underlying the agencies' refusal to disclose the names of uncharged individuals and entities. But the interests of preventing bribe paying – the core objective of the FCPA – should outweigh those legitimate due process concerns and warrant public disclosure of known bribe-paying intermediaries.

See "Making Corporate Transparency a Global Norm" (Sep. 4, 2019).

Identifying Risky Third Parties Could Decrease Corruption

In contrast to a typical criminal case or domestic enforcement action, in the FCPA context, companies and individuals can be and often are charged based on the actions of third-party intermediaries.

Third Parties Present Higher Risks

According to the Stanford Law School FCPA Clearinghouse, in 2019, 15 of the 19 enforcement actions involved bribery schemes that relied on third-party intermediaries. The percentages were even higher in the preceding five years: 100% in 2014 and 2015; 81% in 2016; 87% in 2017; and 89% in 2018.

The U.S. agencies charged with enforcing the FCPA – the DOJ and SEC – have recognized this core truth of FCPA risk, stating in A Resource Guide to the U.S. Foreign Corrupt Practices Act (FCPA Resource Guide): "DOJ's and SEC's FCPA enforcement actions demonstrate that third parties, including agents, consultants, and distributors, are commonly used to conceal the payment of bribes to foreign officials in international business transactions."

Enforcement Agencies Have High Expectations

The agencies have also made clear their expectation that companies know their third-party intermediaries and fully vet them – if not, companies risk failing to qualify as having an effective FCPA and anti-

bribery compliance program and are thus disqualified from obtaining compliance credit in charging decisions and fine and penalty calculations. And the enforcement agencies expect companies to know a lot about their intermediaries, particularly those operating in high bribery risk jurisdictions and interacting with foreign government officials.

In the FCPA Resource Guide, the SEC and DOJ note that "[r]isk-based due diligence is particularly important with third parties and will also be considered by DOJ and SEC in assessing the effectiveness of a company's compliance program." DOJ expands on this point in its 2020 Compliance Guidance:

> A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions. Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials.

See "ECCP Refinements Encourage Companies to Make Compliance a Positive Feedback Loop" (Jun. 24, 2020)

Enforcement Agencies May Be Laying Tripwires for Companies

As the FCPA compliance bar well knows, there is a substantial risk that DOJ and/or the SEC will bring an enforcement action based on the company's willful blindness to the risk of bribery if a company engages an intermediary to engage in high-risk activity on its behalf without conducting adequate due diligence on the business partner and the intermediary ultimately pays a bribe on behalf of the company.

The Bio-Rad Laboratories, Inc. and Alcoa, Inc. cases provide two examples. In Bio-Rad, the DOJ and SEC found that the company paid third-party commissions on its Russian sales knowing that those third parties likely were not capable of performing the services described in their contracts based on red flags the company ignored. Regarding Alcoa, the SEC found that Alcoa subsidiaries either knew or consciously disregarded the high likelihood that "Consultant A" would use his commissions and markup to pay bribes.

The FCPA thus creates tripwires for companies trying to comply with the FCPA that they do not necessarily face when trying to comply with other statutes. This dynamic creates a risk that a company, acting in good faith, could engage a third-party intermediary after having conducted reasonable due diligence but not discovering that the intermediary was in fact "CONSULTING COMPANY A" or "DISTRIBUTOR 2," known by the U.S. government to have previously paid bribes on behalf of a different company. This could lead to the untenable result of an enforcement action against the company based in part on its failure to learn facts already known to the agencies. This "gotcha" result is fundamentally inconsistent

with the goals of the FCPA enforcement paradigm.

This problem would be solved if the DOJ and SEC publicly disclosed the names of known bribe payers – companies and individuals whose conduct formed the basis for FCPA charges against their principals.

Benefits Outweigh Due Process Concerns

The DOJ has taken the position that there is "ordinarily" no need to name a person as an unindicted co-conspirator in an indictment in order to fulfill any "legitimate prosecutorial interest or duty." In the "absence of some significant justification," DOJ will not identify a third-party wrongdoer by name or an "unnecessarily specific description," or cause a defendant to identify a third-party wrongdoer, unless that party has been officially charged with the misconduct at issue.

Thus, in FCPA charging documents, and in the statements of fact accompanying plea agreements, deferred prosecution agreements and other resolutions, bribe-paying intermediaries are referred to in such forms as "Consultant 1," "Cargo Executive," or "Construction Company." While not the subject of a formal policy, the SEC has followed a similar approach, referring to "third parties," "third-party commercial representatives and distributors," or "third-party agents" in civil complaints and resolution orders.

This policy is rooted in due process. As a general rule, law enforcement should not be publicly shaming, and arguably defaming, individuals where there is no sufficient basis to charge them. One court explained that "the liberty and property concepts of the Fifth Amendment protect an individual from being publicly and officially accused of having committed a serious crime, particularly where the accusations gain wide notoriety," and that there is some defamatory element that can be causally attributed to the government.

However, we submit that the interests of preventing bribe paying – the core objective of the FCPA – and of giving companies intent on complying with the law full information about known risks outweigh those legitimate due process concerns and warrant a different treatment in the FCPA context: public disclosure of known bribe-paying intermediaries.

Models for FCPA Bribe-Payer Lists Exist

The public identification of bad actors like bribe-payers is not without precedent in international compliance, as shown by the Specially Designated Nationals (SDNs) list issued by the Office of Foreign Asset Control (OFAC) and the World Bank's Procurement list. OFAC and other government agencies, including the U.S. Commerce Department's Bureau of Industry & Security (BIS), also provide so-called "positive lists" of high-risk parties. Although the statutory authority for and substantive focus of these lists differ, they nonetheless illustrate how agencies can balance due process with the promotion of critical compliance interests. Assuming that the DOJ and SEC want less foreign bribery, they should adopt a similar approach.

DOJ and SEC should develop a bribe-payer blacklist that would promote FCPA compliance by providing companies with critical risk

information while at the same time addressing the due process concerns that underlie the current approach. U.S. government agencies and international institutions have already developed and implemented similar systems that could serve as models.

The World Bank's Procurement Rule Violators List

The World Bank Group's model is a case in point. Under its fraud and corruption policy, the World Bank targets entities and individuals engaged in bribery, corruption, fraud or the misuse of grants and loans. This designation make individuals and entities ineligible for Bank-financed contracts. The World Bank publishes a list of entities that have either violated the Procurement or Consultant Guidelines (for projects prior to July 1, 2016), or the World Bank Procurement Regulations for Investment Project Financing Borrowers (after July 1, 2016). The World Bank also has an administrative process that allows the targeted entity or individual to confront the allegations and provide exculpatory evidence. Although these are not judicial proceedings, they nonetheless address potential due process concerns by providing a meaningful opportunity to be heard. These World Bank procedures could serve as an effective model for a DOJ/SEC bribe-paying intermediary list.

See "The World Bank's Wide Reach and Its Growing Anti-Corruption Program" (May 28, 2014).

OFAC Economic Sanctions Lists

Some U.S. government agencies likewise name uncharged individuals and entities to promote certain compliance interests while also providing due process to those named. For example, OFAC publishes several lists of entities and individuals engaged in activities that threaten U.S. foreign policy or national security interests. Notable examples include terrorist organizations, weapons proliferators, narcotics syndicates and parties owned or controlled by hostile foreign governments. Parties targeted under these sanctions programs include SDNs. U.S. persons are prohibited from engaging in commercial or financial transactions with SDNs, and are required to block (or "freeze") any SDN assets or contracts that come within their control. This approach may appear severe, but the fact that OFAC publishes a searchable list of restricted parties gives companies a clear, objective standard that helps them identify risks, mitigate exposure and comply with U.S. government requirements.

See "Preparing for a Sanctions Crackdown on Apparel Companies with Operations in China" (Oct. 3, 2018).

The BIS Entity List

BIS maintains similar restricted party lists for export control purposes. Chief among them is the Entity List, which identifies foreign parties involved in the proliferation of U.S. products, software or technology to hostile countries and groups. BIS prohibits companies from exporting U.S. products to parties appearing on the Entity List. Like the OFAC sanctions lists, this approach uses party-specific designations to reduce uncertainty and promote compliance in a critical enforcement area.

See "How the Department of Commerce Can Help Companies Address Anti-Corruption and Cybersecurity Concerns" (Oct. 21, 2015).

Listed Parties Could Challenge Designation

Much like the World Bank model, the OFAC and BIS designation processes include certain due process protections. Target entities and individuals have the opportunity to challenge their designation after the fact. More significantly, they may engage legal counsel as advocates in these processes, even in cases where the underlying laws would prohibit other U.S. parties from conducting business with them. These processes provide a mechanism for removing SDNs and other sanctioned parties in circumstances involving cases of mistaken identity or changes in the problematic behavior.

The OFAC and BIS appeal processes are similar. To challenge an OFAC designation, parties must submit a detailed dossier explaining the legal and factual rationale for de-listing. A successful targeted party generally furnishes facts demonstrating that OFAC had an insufficient basis for the designation or made an error during the designation process. In cases where the factual basis for the designation was adequate, petitioners can argue that the circumstances informing the designation no longer apply. Notable examples include the SDN's death or dissolution, changes in U.S. foreign policy or positive changes in behavior (including the designated party's cooperation with U.S. defense, intelligence or law enforcement agencies).

OFAC's denial of a request to de-list an entity or individual from the SDN list constitutes an exhaustion of administrative remedies, which allows entities and individuals to bring an action in federal court seeking judicial review under the Administrative Procedure Act. Although these due process protections are not perfect, they have widely been accepted as legitimate and effective. The majority of courts hearing cases challenging the OFAC SDN process have held that it comports with due process, by providing a meaningful opportunity to be heard and because the SDN designation can be challenged.

BIS manages the Entity List appeals process through its End-User Review Committee (ERC). Parties seeking a removal from the Entity List or a modification of the associated restrictions must file dossiers with BIS describing the legal and factual rationale. The ERC then evaluates the submission and votes on removal or modification, usually within 30 days. Like the OFAC appeals process, there is no limit on the number of times an entity or individual can appeal a BIS Entity List designation.

Thus, other U.S. government enforcement agencies have implemented practical mechanisms for "blacklisting" problematic parties while maintaining processes for correcting, modifying or even reversing such determinations. If these agencies can implement and administer restricted party lists identifying terrorists, proliferators and other high-risk entities, then the DOJ and SEC should be able to adopt a more transparent approach for identifying the third-party intermediaries that have already engaged in bribery or other corrupt conduct.

See "Compliance and Self-Protection in an Uncertain Sanctions Environment" (Nov. 1, 2017).

Bribe-Payers Should Be Named

The primary purpose of the FCPA and the DOJ/SEC FCPA enforcement program is to identify, deter and ultimately prevent bribe paying. These agencies have correctly recognized the fact that bribes are typically paid by and through third-party intermediaries. Expecting U.S. companies to aggressively vet intermediaries who operate in countries that present a high risk of bribery is entirely reasonable. But the DOJ and SEC are both sitting on a database of known bribe-payers, including companies and individuals whose misconduct abroad prompted criminal prosecutions of U.S. companies. And despite collecting that information, they have refused to share it with corporate compliance professionals committed to effective due diligence and avoiding bad actors. This is unfair, unwise and ultimately undermines enforcement program objectives. If the DOJ and SEC are truly committed to supporting informed FCPA compliance programs, then these agencies should publish these names and develop appropriate procedures for named parties to challenge their designation.

David W. Simon, a partner at Foley & Lardner, leads the firm's government enforcement, investigations and compliance international practice. He provides compliance advice, conducts internal investigations, defends companies against enforcement actions and represents companies in litigation. The FCPA and other anti-bribery laws are a principal focus of his practice.

Christopher Swift is a partner and litigator in Foley & Lardner's government enforcement, defense and investigations practice. Drawing on two decades of experience in national security and international law, Swift defends clients in complex enforcement actions involving anti-money laundering, economic sanctions, export controls, cybersecurity and other cross-border risks implicating enhanced government surveillance, intelligence and law enforcement authorities.

Olivia S. Singelmann, a senior counsel at Foley & Lardner, is a litigation attorney who counsels clients on anti-bribery and anti-corruption issues with a focus on Latin America, as well as public company accounting and compliance with public company audit standards. She provides compliance advice, conducts internal investigations, and represents clients in investigations and enforcement proceedings by regulators such as the DOJ and the SEC.

Jenlain A. Scott, an associate at Foley & Lardner, is a litigation attorney who counsels clients on international issues, including anti-dumping proceedings, customs issues and CFIUS national security matters. He also represents clients in internal investigations and commercial litigation.