

Potential FCPA Liability for Third-Party Conduct

ROBERT C. BLUME, JOHN D.W. PARTRIDGE, AND TAFARI NIA LUMUMBA, GIBSON, DUNN & CRUTCHER LLP,
WITH PRACTICAL LAW LITIGATION

Search the [Resource ID numbers in blue](#) on Westlaw for more.

A Practice Note examining key issues for government investigations of alleged Foreign Corrupt Practices Act (FCPA) violations involving corrupt payments made by third parties. This Note discusses Department of Justice (DOJ) and Securities and Exchange Commission (SEC) theories of liability for third-party misconduct, identifies certain high-risk third parties, analyzes relevant third-party enforcement actions, describes the challenges in investigating potential third-party misconduct, and details best practices companies can use to assess third-party risk to prevent improper conduct.

To facilitate the delivery of goods and services to markets across the globe, multinational companies rely on an array of agents, consultants, distributors, and other third parties operating overseas. These third-party business partners provide:

- Local expertise.
- Experience.
- Connections.
- Satisfaction of some jurisdictions' local requirements that foreign companies collaborate with local entities.

However, third parties may bring legal and reputational risk to the companies that engage them. Misconduct by third parties can be more challenging to identify or prevent than misconduct carried out by company employees.

The Foreign Corrupt Practices Act (FCPA) prohibits not only direct corrupt payments to a foreign official to obtain or retain business but also indirect corrupt payments made using third parties. Some of the largest FCPA enforcement actions have involved third-party payments.

Like most FCPA enforcement actions involving corporate entities, FCPA cases premised on third-party liability theories are more commonly settled than litigated. Companies tend to settle FCPA cases to mitigate potential monetary penalties and to avoid the severe collateral consequences that may accompany criminal conviction. Because so few companies put the government to its proof, case law on the government's third-party liability theories is sparse.

With few court-imposed bounds and plenty of potentially suspect business arrangements, the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) have been increasingly attuned to complex schemes involving third parties that act as conduits for improper payments. In light of this scrutiny and the need to rely on third parties in many parts of the world, the risks and rewards of engaging third-party business partners are significant. Balancing those risks and rewards requires an understanding of how the FCPA applies to third-party conduct. This Note explains the potential liability for third-party misconduct under the FCPA.

FCPA: OVERVIEW

The FCPA contains two sets of provisions:

- Anti-bribery.
- Accounting.

These provisions work in concert to impose liability on certain individuals and entities that engage in foreign bribery or fail to either maintain accurate books and records or adopt prophylactic accounting controls.

For information on the FCPA generally, see Practice Note, The Foreign Corrupt Practices Act: Overview ([0-502-2006](#)).

ANTI-BRIBERY PROVISIONS

Prohibited Conduct

The FCPA's anti-bribery provisions make it illegal for certain individuals and entities to:

- Make, offer, promise, or authorize corrupt payments or transfer anything else of value to foreign officials to obtain or retain business.

- Offer, give, or authorize the transfer of anything of value to “any person, while knowing that all or a portion of such . . . thing of value will be offered, given, or promised directly or indirectly, to any foreign official” to obtain or retain business.

(15 U.S.C. §§ 78dd-1, 78dd-2, and 78dd-3.)

The FCPA therefore can ensnare individuals or companies that directly or indirectly provide anything of value to foreign government officials.

Covered Individuals and Entities

The individuals and entities covered by the FCPA’s anti-bribery provisions are:

- **Issuers.** Companies that have securities registered with the SEC or must file periodic reports with the SEC (15 U.S.C. § 78dd-1). This includes foreign companies that list American Depositary Receipts on US stock exchanges (see, for example, *In re: Astrazeneca PLC*, Admin. Proc. File No. 3-17517 (Aug. 30, 2016)).
- **Domestic concerns.** Natural persons who are US citizens, nationals, or residents and business entities that have their principal place of business in the US or that are organized under the laws of a US state, territory, possession, or commonwealth (15 U.S.C. § 78dd-2).
- **Certain persons acting within US territory.** Any person who uses US mail or any means or instrumentality of interstate commerce or does any other act while in US territory in furtherance of prohibited conduct (15 U.S.C. § 78dd-3). In practice:
 - an instrumentality of interstate commerce includes telephone calls, faxes, emails, and travel, as well as interstate and international bank wire transfers (DOJ and SEC, A Resource Guide to the US Foreign Corrupt Practices Act, at 11 (Nov. 14, 2012) (FCPA Resource Guide)); and
 - an act in furtherance applies to a range of activities associated with any misconduct. For example, the DOJ invoked US jurisdiction based on a company’s transmission to the US of an email attaching a budget document that contained a line item for improper payments to foreign officials (*Information ¶¶ 15-17, United States v. Syncor Taiwan, Inc.*, No. 2:02-cr-1244 (C.D. Cal. Dec. 5, 2002)).

The anti-bribery provisions apply not only to an issuer or domestic concern itself but also to any officer, director, employee, agent, or stockholder that acts on behalf of the covered individual or entity (15 U.S.C. §§ 78dd-1, 78dd-2, and 78dd-3).

ACCOUNTING PROVISIONS

Required Conduct

The FCPA’s accounting provisions require that issuers:

- Make and keep books, records, and accounts that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets.
- Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that unauthorized payments are not made and that the issuer can prepare financial statements according to generally accepted accounting principles.

(15 U.S.C. § 78m(b)(2).)

Covered Entities

The entities covered by the FCPA’s accounting provisions include:

- **Issuers.** Issuers may be held criminally or civilly liable for their own failures and for those of other entities they control, such as:
 - subsidiaries;
 - joint ventures; and
 - affiliates.
- Where an issuer controls more than 50% of the voting power of a non-issuer entity, it can be held liable for that entity’s failures to comply with the FCPA’s books-and-records and internal accounting controls requirements. Where an issuer holds 50% or less of the entity’s voting power, it must only “proceed in good faith to use its influence, to the extent reasonable under the issuer’s circumstances, to cause the entity to devise and maintain a system of internal controls consistent with” the FCPA’s accounting provisions. (15 U.S.C. § 78m(b)(6) and see Joint Venturers.)
- **Non-issuers.** Officers, directors, and subsidiaries of an issuer may be held criminally or civilly liable if they:
 - knowingly circumvent or knowingly fail to implement a system of internal accounting controls (15 U.S.C. § 78m(b)(5));
 - knowingly falsify any book, record, or account (15 U.S.C. § 78m(b)(5)); or
 - directly or indirectly falsify or cause to be falsified an issuer’s books and records (17 C.F.R. § 240.13b2-1).

RED FLAGS

The FCPA Resource Guide identifies red flags associated with third parties, including:

- Excessive commissions to third-party agents or consultants.
- Unreasonably large discounts to third-party distributors.
- Third-party consulting agreements that include only vaguely described services.
- Third-party consultants that are in a different line of business than that for which they are being engaged.
- Third parties related to or closely associated with a foreign official.
- Third parties that became part of a transaction at the express request or insistence of a foreign official.
- Third parties that are merely shell companies incorporated in an offshore jurisdiction.
- Third parties that requested payment to offshore bank accounts. (FCPA Resource Guide, at 22-23.)

For more information about the FCPA Resource Guide, see Legal Update, New FCPA Guidance Released by the DOJ and SEC ([6-522-4695](#)).

THEORIES OF LIABILITY: ANTI-BRIBERY PROVISIONS

The government commonly pursues FCPA enforcement actions against companies based on the conduct of their third-party business partners under the theories of:

- Direct participation (see Direct Participation in Third-Party Misconduct).
- Authorization (see Authorization of Third-Party Misconduct).

- Knowledge (see Knowledge of Third-Party Misconduct).
- Agency (see Agency).
- Aiding and abetting (see Aiding and Abetting).
- Conspiracy (see Conspiracy).

DIRECT PARTICIPATION IN THIRD-PARTY MISCONDUCT

The government may target a company for the corrupt acts of third parties if the company participated in the third parties' improper conduct. Participation could include directing an agent's misconduct. (FCPA Resource Guide, at 27.)

For example, in 2011, Magyar Telekom PLC, a Hungarian telecommunications company and an issuer, and its majority owner agreed to pay more than \$95 million, without admitting or denying the allegations, to resolve DOJ and SEC charges that it directly participated in a bribery scheme through a third party. According to the SEC's complaint, executives at Magyar Telekom orchestrated, approved, and executed a plan to bribe Macedonian government officials to obtain favorable regulatory changes and prevent a new competitor from entering the market. The SEC further alleged that executives at Magyar Telekom caused the company's subsidiaries in Macedonia to pay at least €4.875 million to a third party under a series of sham marketing and consulting contracts. The third party then purportedly forwarded the money to government officials. (Complaint ¶¶ 2, 15, 22, *SEC v. Magyar Telekom plc.*, No. 11-cv-9646 (S.D.N.Y. Dec. 29, 2011) and Press Release, SEC, SEC Charges Magyar Telekom and Former Executives with Bribing Officials in Macedonia and Montenegro (Dec. 29, 2011).)

AUTHORIZATION OF THIRD-PARTY MISCONDUCT

The FCPA's anti-bribery provisions prohibit the authorization of the payment of any money or the giving of anything of value for the purpose of obtaining, retaining, or directing business (15 U.S.C. §§ 78dd-1(a), 78dd-2(a), and 78dd-3(a)). Although the FCPA does not define authorization, the statute's legislative history indicates that authorization can be either express or implied (H.R. Rep. No. 95-640, at 8 (1977)). The government has asserted that a company is liable for FCPA violations if it provides something of value to a third party while aware or substantially certain that the third party will offer, give, or promise something of value to a foreign official (see Knowledge of Third-Party Misconduct).

For example, the SEC's July 2014 settlement with Smith & Wesson Holding Corporation involved both express and implied authorization allegations. Smith & Wesson agreed to pay \$2 million to settle charges that it authorized third-party agents to pay foreign officials to win government contracts to supply its products to law enforcement and military departments. According to the SEC, to try to win government contracts, Smith & Wesson employees made payments to the agents even though the agents indicated that they would send some of the funds to public officials. For example, the SEC alleged that the company made payments to an agent in Indonesia after the agent explained that the police officials expected to be paid to enter into a contract with the company. The agent allegedly informed the company that portions of the payment the agent would receive from the company would be given to police officials. The SEC asserted that the company impliedly authorized the payments because it was aware that the agent made the

payments to the officials by paying an inflated amount above the actual cost for legitimate gun-testing services the police department performed. The Indonesian deal was never consummated. The SEC also asserted that the company expressly authorized its agent to proceed after the agent informed the company that he would provide cash and guns to Pakistani police officers to close the deal. The SEC characterized Smith & Wesson's employee as "knowing or consciously disregarding" that the agent would be providing the guns and part of his commissions to the officials as an inducement to enter into the deal. Smith & Wesson settled the charges without admitting or denying the SEC's findings. This case also illustrates the government's willingness to pursue cases under an authorization theory even if the conduct at issue resulted in only modest profits. (*In re: Smith & Wesson Holding Corp.*, Admin. Proc. File No. 3-15986 (July 28, 2014).)

KNOWLEDGE OF THIRD-PARTY MISCONDUCT

The FCPA defines "knowing" as either:

- Awareness that a third party is engaging in misconduct or substantially certain that the third party will engage in misconduct.
- A firm belief that a third party is engaging in misconduct or substantially certain that the third party will engage in misconduct. (15 U.S.C. § 78dd-2(h)(3)(A)(i), (ii).)

The government may establish knowledge by showing that the defendant was aware of a "high probability of the existence" of that conduct, unless the defendant "actually believe[d]" the conduct was not occurring (15 U.S.C. § 78dd-2(h)(3)(B)).

The government contends that the FCPA not only imposes liability on those with actual knowledge of wrongdoing but also on those who purposefully avoid actual knowledge (FCPA Resource Guide, at 22). Courts have agreed and construed knowing to include deliberate ignorance (also referred to as willful blindness or conscious avoidance) (see *United States v. King*, 351 F.3d 859, 867 (8th Cir. 2003) (approving a deliberate ignorance jury instruction in an FCPA prosecution)).

For example, in *United States v. Kozeny*, the US Court of Appeals for the Second Circuit affirmed Frederic Bourke's conviction for conspiring to violate the FCPA. Bourke's business partner, Viktor Kozeny, allegedly channeled millions of dollars to Azeri officials to persuade them to privatize Azerbaijan's state-owned oil company and sell the entity to Bourke and his investors. Bourke denied any knowledge of Kozeny's payments, and the district court instructed the jury that Bourke had the requisite knowledge of payments under the FCPA if he was aware of a high probability that corrupt payments were being made but consciously and intentionally avoided confirming that fact.

On appeal, the court concluded that the government presented sufficient evidence of Bourke's conscious avoidance. The government established that Bourke:

- Knew that Kozeny, the scheme's mastermind, had a reputation for corrupt business conduct and that Azeri officials would ultimately receive an ownership stake in the oil company if it were privatized.
- Contacted his attorneys to discuss ways to limit his potential FCPA liability.

- Formed American advisory companies to shield him and other American investors from potential liability for improper payments under the FCPA.

(*United States v. Kozeny*, 667 F.3d 122, 127-133 (2d Cir. 2011).)

The government also uses these theories against corporate entities. For example, in 2014, the DOJ and the SEC announced FCPA resolutions with California-based medical device company Bio-Rad Laboratories, Inc. to settle charges that its foreign agents paid bribes to secure government contracts. In recognition of, among other things, Bio-Rad's voluntary disclosure and cooperation, the DOJ entered into a non-prosecution agreement (NPA) with Bio-Rad (DOJ Non-prosecution Agreement, Bio-Rad Laboratories, Inc. (Nov. 3, 2014)).

According to the SEC, between 2005 and 2010, a Bio-Rad subsidiary paid third parties 15% to 30% commissions on its Russian sales knowing that the third parties likely did not have the capability to perform the services described in their contracts. The Bio-Rad subsidiary paid the third parties \$4.6 million on sales of \$38.6 million.

The SEC asserted that executives at the parent company ignored red flags that allowed the scheme to continue for years, including that:

- The third parties were not located in Russia.
- The third parties did not have the resources to perform the contracted-for services.
- The subsidiary paid excessive commissions to banks in Latvia and Lithuania.
- The third parties made efforts to keep the payments secret.
- The services were not necessary to the company's business.

(*In re: Bio-Rad Labs., Inc.*, Admin. Proc. File No. 3-16231 (Nov. 3, 2014) and Press Release, DOJ, Bio-Rad Laboratories Resolves Foreign Corrupt Practices Act Investigation and Agrees to Pay \$14.35 Million Penalty (Nov. 3, 2014).)

AGENCY

Companies may be held liable for a third party's FCPA violations under traditional agency principles. Under the principle of respondeat superior, a company is liable for the acts of its agents, including the acts of its officers and employees:

- Undertaken within the scope of their agency relationship.
- Intended at least in part to benefit the company.

In these situations, the agent's actions and knowledge may be imputed to the principal. The government is not required to prove the principal's independent knowledge or corrupt intent. (FCPA Resource Guide, at 27.)

To determine whether a third party qualifies as a covered entity's agent, the government focuses on the extent of control by the covered entity over the third party. The government factors in the company's knowledge and direction of the third party's actions both generally and in the context of the specific actions under investigation. A formal relationship between the covered entity and the third party is one key factor in the agency analysis, but the DOJ and the SEC also consider the practical realities of how the two entities interact. (FCPA Resource Guide, at 27-28.)

The government has asserted that various types of third parties were agents of defendant companies, including foreign:

- Subsidiaries (see, for example, Information ¶ 1, *United States v. DPC (Tianjin) Co. Ltd.*, No. 2:05-cr-00482 (C.D. Cal. 2005) and *In re: Alcoa Inc.*, Admin. Proc. File No. 3-15673 (Jan. 9, 2014)).
- Consultants (see, for example, *In re: Alcoa Inc.*, Admin. Proc. File No. 3-15673 (Jan. 9, 2014)).
- Attorneys (see, for example, Press Release, DOJ, UK Solicitor Pleads Guilty for Role in Bribing Nigerian Government Officials as Part of KBR Joint Venture Scheme (Mar. 11, 2011)).

In the *Alcoa* enforcement action, the SEC alleged that Alcoa Inc. violated the FCPA because of the conduct of a non-issuer subsidiary, which purportedly acted as Alcoa's agent and, in that capacity, made improper payments to foreign officials. To support the agency theory, the SEC asserted Alcoa exhibited control over the subsidiary because:

- Alcoa appointed the majority of the subsidiary's strategic council.
- Alcoa set the business and financial goals and coordinated legal, audit, and compliance for the subsidiary.
- The subsidiary's employees in the business area relevant to the investigation reported to Alcoa personnel.

Alcoa settled with the SEC and agreed to disgorge more than \$175 million in ill-gotten gains. (*In re: Alcoa Inc.*, Admin. Proc. File No. 3-15673 (Jan. 9, 2014).)

AIDING AND ABETTING

Under federal law, individuals or companies that aid or abet a crime are considered as culpable as if they had directly committed the crime. The government must prove that:

- A crime was committed by someone other than the defendant.
- Before or at the time the crime was committed, the defendant:
 - aided;
 - counseled;
 - commanded;
 - induced; or
 - procured the person who committed the crime.
- The defendant intended to facilitate the crime.

(18 U.S.C. § 2; see US Attorneys' Criminal Resource Manual § 2474.)

Generally, the "defendant must share the principal's criminal intent and engage in some affirmative conduct designed to aid the venture" (*United States v. Gallo*, 927 F.2d 815, 822 (5th Cir. 1991)). Since aiding and abetting is not an independent crime, the government also must prove that a substantive FCPA violation occurred.

CONSPIRACY

In contrast to aiding and abetting, conspiracy is an independent crime. Individuals and companies can be held liable for conspiring to violate the FCPA, even if they cannot be charged with a substantive FCPA violation.

A conspiracy under 18 U.S.C. § 371 requires the government to prove:

- An agreement between two or more persons to achieve a common objective.

- The objective of the agreement is illegal.
- The defendant's knowing and voluntary participation in that common agreement.
- Any conspirator's commission of an overt act in furtherance of the illegal objective.

(See *United States v. Snype*, 441 F.3d 119, 142 (2d Cir. 2006).)

The agreement does not have to be written, oral, or explicit and may be inferred from facts and circumstances (see, for example, *Iannelli v. United States*, 420 U.S. 770, 777 n.10 (1975) and *United States v. Amiel*, 95 F.3d 135, 144 (2d Cir. 1996)).

In criminal cases, entities can conspire with their employees, officers, agents, or other individuals or entities associated with it (see *United States v. Hughes Aircraft Co.*, 20 F.3d 974, 978-79 (9th Cir. 1994) and *United States v. Peters*, 732 F.2d 1004, 1008 (1st Cir. 1984)). However, there must be at least two individuals involved in the conspiracy for a conspiracy charge. An employee, acting alone on the entity's behalf, cannot conspire with the corporation. (See *United States v. Sain*, 141 F.3d 463, 475 (3d Cir. 1998) and *Peters*, 732 F.2d at 1008 n.6.)

In certain types of civil conspiracy cases, some courts apply the Intracorporate Conspiracy Doctrine, which holds that an entity cannot conspire with its employees, officers, agents, or other individuals or entities associated with it (see, for example, *Pizza Mgmt. Inc. v. Pizza Hut, Inc.*, 737 F. Supp. 1154, 1165-66 (N.D. Ill. May 11, 1990)). Some courts have refused to apply the doctrine to certain types of claims (see *Stathos v. Bowden*, 728 F.2d 15, 20-21 (1st Cir. 1984) (refusing to apply the doctrine in a civil rights action) and *Ashland Oil, Inc. v. Arnett*, 875 F.2d 1271, 1281 (7th Cir. 1989) (refusing to apply the doctrine in a RICO action)).

The overt act does not need to be a criminal act or even a substantial one. Any step in preparation that is helpful to the agreement's objective can satisfy the requirement (see, for example, *Iannelli*, 420 U.S. at 786 n.17 (observing that the overt act "can be innocent in nature, provided it furthers the purpose of the conspiracy") and *United States v. Khamis*, 674 F.2d 390, 393 (5th Cir. 1982) (holding that opening bank accounts met the overt act requirement)).

In the government's eyes, a conspiracy charge widens the FCPA's jurisdictional net. According to the DOJ and the SEC, "in conspiracy cases, the United States generally has jurisdiction over all the conspirators where at least one conspirator is an issuer, domestic concern, or commits a reasonably foreseeable overt act within the United States." The DOJ and the SEC also contend that foreign companies that are not issuers "may be subject to substantive FCPA charges under Pinkerton liability, namely, being liable for the reasonably foreseeable substantive FCPA crimes committed by a co-conspirator in furtherance of the conspiracy." (FCPA Resource Guide, at 12, 34.)

The exposure to punishment under FCPA conspiracy charges can be just as significant as under the statute's substantive provisions. For example, in December 2016, Rolls-Royce plc entered into a deferred prosecution agreement (DPA) with the DOJ and agreed to pay nearly \$170 million as a criminal penalty to resolve FCPA violations. Rolls-Royce admitted to conspiring to violate the FCPA by paying bribes through third parties to foreign officials in multiple countries to receive confidential information and contracts. In related

proceedings, Rolls-Royce settled with the UK's Serious Fraud Office and the Brazilian Ministério Público Federal. In total, Rolls-Royce agreed to pay more than \$800 million in criminal penalties. (Press Release, DOJ, Rolls-Royce plc Agrees to Pay \$170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case (Jan. 17, 2017).)

THEORIES OF LIABILITY: ACCOUNTING PROVISIONS

CONDUCT OF ISSUER

Issuers can be held liable for failing to comply with the FCPA's:

- **Books-and-records provisions.** Issuers must appropriately and accurately record payments to third parties, such as agents, consultants, and distributors (see, for example, discussion of *United States v. Alstom S.A.* in Local Sales Agents and Consultants).
- **Internal controls provisions.** Issuers must implement and maintain internal controls to mitigate third-party risks (see, for example, discussion of *SEC v. Technip* in Joint Venturers).

CONDUCT OF ISSUER'S SUBSIDIARY

Issuers also can be held directly liable for the failures of their subsidiaries to comply with the FCPA's:

- **Books-and-records provisions.** Issuers must oversee their subsidiaries' compliance with the FCPA's accounting provisions.
- **Internal controls provisions.** Issuers must ensure that their subsidiaries implement and maintain adequate internal controls.

(See, for example, *In re: Alcoa Inc.*, Admin. Proc. File No. 3-15673 (Jan. 9, 2014), discussion of the *Alcoa* enforcement action in Agency, *In re: Bio-Rad Labs., Inc.*, Admin. Proc. File No. 3-16231 (Nov. 3, 2014), and discussion of the *Bio-Rad* enforcement action in Knowledge of Third-Party Misconduct.)

HIGH-RISK THIRD PARTIES

Certain categories of third parties can present more significant corruption risks, including:

- Sales agents and consultants (see Local Sales Agents and Consultants).
- Distributors (see Distributors).
- Freight forwarders (see Freight Forwarders).
- Customs brokers and customs agents (see Customs Agents and Customs Brokers).
- Joint venturers (see Joint Venturers).

For more information on these high-risk third parties generally, see Practice Note, Supply Chain Overview: Supply Chain Participants and Their Key Functions ([0-523-6390](#)) and Box: Strategic Alliances and the Supply Chain ([0-523-6390](#)).

LOCAL SALES AGENTS AND CONSULTANTS

Companies operating overseas often rely on local sales agents and consultants to open doors and complete deals. Local sales agents and consultants can provide:

- In-country personnel with local language skills.
- Insight regarding customers':

- decision-makers;
- tender processes;
- technical specifications;
- needs; and
- expectations.

For these contributions, local sales agents and consultants receive compensation, which is often tied, directly or indirectly, to successful sales, which may lead to misconduct.

Red Flags

The FCPA Resource Guide details several consultant-specific corruption red flags, such as:

- Excessive commissions, which may be used to make improper payments.
- Consulting agreements that include only vaguely described services, which may attempt to cover up improper payments.
- Third-party consultants operating in different lines of business than their engagement, which may suggest that the consultants cannot perform the services retained and instead were hired to make improper payments.

(FCPA Resource Guide, at 22-23.)

Case Example

In December 2014, Alstom S.A., a French power company, and several of its subsidiaries agreed to pay \$772 million to resolve allegations that Alstom paid approximately \$75 million to third-party consultants to secure more than \$4 billion worth of projects in the Bahamas, Egypt, Indonesia, Saudi Arabia, and Taiwan, while knowing that at least a portion of the consultant payments would be used to bribe foreign officials in those nations. According to the DOJ's criminal information, Alstom and its subsidiaries attempted to conceal the bribery scheme by:

- Hiring third parties to provide sham consulting services.
- Recording the third-party payments as consultancy fees or commissions in its books and records.

The DOJ focused on the alleged inadequate due diligence Alstom conducted on the consultants, despite several red flags, such as the consultants':

- Lack of relevant experience.
- Provision of duplicative services.
- Demand to be paid in a different country or currency.
- Location in a country other than where they were to perform the services.

(Press Release, DOJ, Alstom Pleads Guilty and Agrees to Pay \$772 Million Criminal Penalty to Resolve Foreign Bribery Charges (Dec. 22, 2014) and Information, ¶¶ 31, 56, 93, *United States v. Alstom Grid, Inc.*, No. 14-cr-247 (D. Conn. Dec. 22, 2014).)

DISTRIBUTORS

Distributors typically purchase products from a company and resell the products in local markets. Depending on the terms of the agreement, a distributor's responsibilities, other than reselling, may include:

- Promotion.
- Marketing.
- Logistics.

Distributors are commonly involved in arm's length transactions of:

- A purchase from the product's manufacturer.
- A sale to the ultimate customer.

For more information on distributors generally, see Practice Note, Distributors and Dealers ([8-500-4225](#)). For sample agreements between a manufacturer and a distributor, see Standard Documents, Distribution Agreement (Pro-Seller, Short Form) ([4-617-9462](#)) and Exclusive Distribution Agreement (Pro-Distributor, Short Form) ([W-002-7704](#)).

Red Flag

The distributor earns a profit on the margin, which is the difference between what it paid to the manufacturer and what it charged the customer. If the manufacturer prices its products at an artificially low level, the distributor may be able to maintain its profit margins on sales to customers while retaining an additional sum that could be used for improper payments. Given this dynamic, the government considers unreasonably large discounts to third-party distributors a corruption red flag because it suggests that the manufacturer deliberately sold its products at a price point that would give the distributor funds to use for improper payments. (FCPA Resource Guide, at 22, 64.)

Although the government views discounts with suspicion, price reductions are commonplace and can appropriately compensate distributors for their legitimate promotional, marketing, or logistical activities. Companies should assess whether a particular discount increases the risk or appearance of improper payments.

Case Examples

In 2016, Teva Pharmaceutical Industries Ltd. agreed to pay a \$283 million criminal penalty and more than \$236 million in disgorgement and interest to resolve allegations by the DOJ and the SEC. Among other alleged misconduct, Teva purportedly made improper payments to government officials in Mexico and Russia through distributors.

According to the SEC's complaint, Teva's Mexican subsidiary gave improper discounts to a distributor to create a margin of cash that could be paid to doctors at government-owned hospitals and clinics to influence their prescribing decisions. Although Teva had an anti-corruption policy in place requiring its subsidiaries to perform due diligence on distributors and obtain a signed anti-corruption acknowledgement form from the distributor, the subsidiary purportedly failed to fulfill either requirement for the distributor at issue.

The SEC's complaint also contended that Teva's Russian subsidiary made payments to a distributor owned by a Russian official in exchange for the official's influence with government procurements. The SEC alleged that Teva worked with the Russian distributor despite:

- Knowing that the distributor's president was being investigated in Russia for making improper payments to government officials.

- Documented concerns about the transparency of the distributor's ownership structure, including indications that a Russian official participated in the business.

(Press Release, SEC, Teva Pharmaceutical Paying \$519 Million to Settle FCPA Charges (Dec. 22, 2016) and Complaint, *SEC v. Teva Pharmaceuticals Ltd.*, No. 1:16-cv-25298 (S.D. Fla. Dec. 22, 2016).)

Notably, the government's allegations about the Mexican distributor track the standard distributor liability theory (inflated margins to create a fund for improper payments), but the allegations regarding the Russian distributor focus on payments to a Russian official associated with the distributor.

In 2015, Illinois-based Mead Johnson Nutrition Company, one of the world's largest manufacturers of infant formula, agreed to pay \$12 million to resolve SEC allegations that it violated the FCPA's accounting provisions. The SEC alleged that between 2008 and 2013 certain employees of Mead Johnson's Chinese subsidiary improperly paid health care professionals at Chinese government-owned hospitals to recommend Mead Johnson's infant formula to new and expectant mothers. The funding for these payments allegedly came from funds generated by the subsidiary providing discounts to third-party distributors who were contracted to market and sell the company's products in China. Although the illicit payments came from funds belonging to the distributors, the SEC contended that the subsidiary's employees provided guidance to the distributors on how to use the funds and retained some control over how the distributors spent the funds. Mead Johnson settled the charges without admitting or denying the SEC's findings. (Press Release, SEC, SEC Charges Mead Johnson Nutrition With FCPA Violations (July 28, 2015) and *In re: Mead Johnson Nutrition Co.*, Admin. Proc. File No. 3-16704 (July 28, 2015).)

FREIGHT FORWARDERS

Freight forwarders act as agents to move cargo for companies. Freight forwarders also advise companies about:

- Import rules.
- Available shipping methods.
- The required documentation for transporting cargo in international trade.

(US Commercial Service, *A Basic Guide to Exporting*, at 221.)

For more information on freight forwarders generally, see Practice Note, *Logistics: Freight Forwarding* ([6-564-7925](#)). For a sample freight forwarding agreement, see Standard Document, *Freight Forwarding Agreement* ([0-603-7525](#)).

Red Flags

Red flags when retaining freight forwarders include:

- Requests for success fees, that is, a premium paid for navigating cargo through foreign territories. Compensation arrangements based on success fees can encourage a freight forwarder to make improper payments to government officials to ensure that cargo gets through, which ensures the freight forwarder earns a fee.
- Relationships between the freight forwarder or its executives and customs personnel in the local jurisdiction.

- Flat fees for the freight forwarder's services without invoices supporting the fees. This may provide freight forwarders an unreasonably high margin that could provide extra funds for bribes.
- Unorthodox payment requests, including that payments be made:
 - in cash; or
 - by wire transfers to shell companies.
- False, duplicative, or inflated invoices.
- Poor reputation or inexperience in the local market.

Case Examples

In November 2013, the DOJ and the SEC announced a joint FCPA resolution with Weatherford International Ltd., a Swiss oil services provider. According to the DPA, a Weatherford subsidiary used a freight forwarding company to funnel bribes to an African foreign official in exchange for the renewal of an oil services contract. Weatherford and the freight forwarder generated sham purchase orders and invoices for services that the third party never performed. When paid for those invoices, the freight forwarding company passed at least some of the money on to the foreign official with the authority to approve Weatherford's contract renewal. As part of the resolution, the company agreed to cooperate with the authorities, retain a compliance monitor for 18 months, and pay more than \$250 million in criminal fines, disgorgement, and civil penalties to the DOJ, SEC, and other government agencies. (See Press Release, SEC, SEC Charges Weatherford International With FCPA Violations (Nov. 26, 2013) and Press Release, DOJ, Three Subsidiaries of Weatherford International Limited Agree to Plead Guilty to FCPA and Export Control Violations (Nov. 26, 2013).)

The government also seeks to hold the freight forwarders liable. In 2010, the DOJ filed a criminal information against Panalpina World Transport (Holding) Ltd., an international freight forwarding and customs clearance company (Information, *United States v. Panalpina World Transport (Holding) Ltd.*, No. 10-cr-769 (S.D. Tex. Nov. 4, 2010)). The DOJ also filed a criminal information against Panalpina World Transport's US-based subsidiary, Panalpina, Inc. (Information, *United States v. Panalpina, Inc.*, No. 10-cr-765 (S.D. Tex. Nov. 4, 2010)). Jurisdiction against Panalpina World Transport was based on an email from a Panalpina, Inc. employee to a Panalpina World Transport employee in Switzerland and a conference call among Panalpina, Inc. employees in the US and Panalpina World Transport employees in Switzerland (Information ¶ 57(a)-(b), *United States v. Panalpina World Transport (Holding) Ltd.*, No. 10-cr-769 (S.D. Tex. Nov. 4, 2010)). The SEC also filed a complaint against Panalpina, Inc. (Complaint, *SEC v. Panalpina, Inc.*, No. 4:10-cv-4334 (S.D. Tex. Nov. 4, 2010)).

The charges against Panalpina, Inc. included that it aided and abetted violations of the FCPA's books-and-records and internal controls provisions. While Panalpina World Transport and Panalpina, Inc. were not issuers, the government alleged that Panalpina, Inc. paid bribes on behalf of its customers, who were issuers. The government also alleged that Panalpina World Transport subsidiaries and affiliates invoiced certain payments to their customers with descriptions intended to aid the customers in concealing bribes to foreign officials in their books, records, and accounts. The alleged improper payments were described using

terms such as “local processing” and “special handling” fees when Panalpina, Inc. and the customers knew the payments were bribes to government officials to garner preferential customs, duties, and import treatment for international shipments. Under the terms of Panalpina World Transport’s DPA and Panalpina, Inc.’s plea agreement, the companies agreed to pay a \$70.56 million total fine and Panalpina, Inc. paid more than \$11 million to settle the SEC’s charges. The investigation and resolutions led the DOJ and SEC to pursue FCPA charges against several multinational companies that used Panalpina World Transport’s services. (See Press Release, DOJ, Oil Services Companies and a Freight Forwarding Company Agree to Resolve Foreign Bribery Investigations and to Pay More Than \$156 Million in Criminal Penalties (Nov. 4, 2010) and *SEC v. Panalpina, Inc.*, Litigation Release No. 21727, 2010 WL 4363894 (Nov. 4, 2010).)

CUSTOMS AGENTS AND CUSTOMS BROKERS

Customs agents and customs brokers typically assist companies with transactions related to the entry of merchandise into foreign countries, including the payment of any duties, taxes, or other charges related to the merchandise’s entry. For more information on customs brokers, see Practice Note, Logistics: Transportation Service Providers Overview: Customs Brokers ([0-525-9268](#)).

Red Flags

The FCPA Resource Guide identifies as red flags a customs agent or customs broker’s:

- Request for excessive commissions.
- Ties to customs officials.

Additional red flags include:

- Success fees for navigating cargo through customs.
- Flat fees without invoices supporting payment.
- Contractual agreements that vaguely describe the work to be performed.

Case Example

In 2014, Layne Christensen Company, a Texas-based construction and drilling company, agreed to pay more than \$5.1 million to resolve allegations that it violated the FCPA’s anti-bribery and accounting provisions. The SEC alleged that, among other unlawful conduct, Layne Christensen made improper payments to customs officials in Burkina Faso and the Democratic Republic of Congo through third-party customs clearing agents. According to the SEC, Layne Christensen made the payments to avoid paying customs duties and to obtain clearance for the import and export of equipment in these countries. A Layne Christensen executive allegedly approved many of these payments without questioning:

- The need to retain the agent.
- The identity of the agent.
- The nature of the services provided.
- The size of the commissions.

The SEC also alleged that the company’s subsidiary inaccurately recorded these payments as legitimate expenses relating to customs and clearance in its books and records. Layne Christensen settled the charges without admitting or denying the SEC’s findings. (Press Release, SEC, SEC Charges Texas-Based Layne Christensen

Company With FCPA Violations (Oct. 27, 2014) and *In re: Layne Christensen Company*, Admin. Proc. File No. 3-16216 (Oct. 27, 2014).)

JOINT VENTURERS

Joint ventures are business undertakings by two or more persons or entities. Joint ventures may be structured in many ways, resulting in various degrees of control for each joint-venture partner, for example:

- A jointly owned company.
- A partnership.
- A limited liability company.

For more information on joint ventures generally, see Practice Note, Joint Ventures: Overview ([0-380-9579](#)).

The government can hold liable for FCPA violations:

- The joint venture.
- The US company or individual that is a party to the joint venture.
- The directors on the joint venture’s board (see Directors).

If a joint-venture participant is an issuer, the degree of the issuer’s control over the joint venture determines its potential exposure under the FCPA’s accounting provisions. An issuer that holds more than 50% of the voting power of another entity can be liable for violations of the FCPA’s accounting provisions.

However, if the joint-venture partner that is the issuer has 50% or less control, then it must only “proceed in good faith to use its influence, to the extent reasonable under the issuer’s circumstances, to cause [the joint venture] to devise and maintain a system of internal accounting controls consistent with [the FCPA’s requirements].” The FCPA notes that relevant factors in assessing the issuer’s circumstances include:

- The relative degree of the issuer’s ownership of the domestic or foreign entity.
- The laws and practices governing the business operations of the country in which the entity is located.

The FCPA further provides that “[a]n issuer which demonstrates good faith efforts to use such influence shall be conclusively presumed to have complied with the requirements of” the accounting provisions. The FCPA does not define good faith. (15 U.S.C. § 78m(b)(6).) Although the FCPA focuses on an issuer’s percentage of voting power, the good faith presumption may not apply if an issuer effectively controls the joint venture and can require it to comply with the accounting provisions (see, for example, *In re: BellSouth Corp.*, Admin. Proc. File No. 3-10678 (Jan. 15, 2002)).

Common Joint Ventures

Common joint ventures include joint ventures with:

- **State-owned companies.** Joint ventures with state-owned enterprises (SOEs) are common in countries where the government dominates certain markets or resources. For example, in the oil industry, a US company may be required to partner with an SOE to tap oil deposits the state controls. Various markets in China similarly require partnerships with local companies.
- **Foreign private companies.** Companies often partner with foreign private businesses because the local entity may have market knowledge, contacts, or infrastructure that makes a joint venture

more advantageous than starting from scratch. Companies might also be obligated or highly incentivized to partner with foreign private companies to access certain markets in a foreign jurisdiction. For example, in Brazil, companies participating in public bids often partner with local Brazilian companies to satisfy rules requiring that a certain percentage of the contract be executed with Brazilian labor and resources. Although foreign private enterprises may not have the same proximity to foreign government officials as SOEs, companies should still vet foreign private companies':

- relationships with local government officials, including their board members' relationships;
- commissions paid to agents;
- discounts given to distributors; and
- compliance with the FCPA and local anti-corruption laws.

Regardless of whether a joint venture involves an SOE or a foreign private entity, various participants in the venture and the joint venture itself can be liable for violating the FCPA, conspiring to do so, or aiding and abetting FCPA violations (see Theories of Liability: Anti-Bribery Provisions).

Case Example

Between 2009 and 2011, the DOJ and the SEC settled anti-bribery and accounting provision charges with four companies participating in a joint venture. Each company owned 25% of the joint venture. The government alleged, among other things, that the joint venture used agents to bribe Nigerian government officials to obtain construction contracts. The SEC's complaint against Technip, one of the joint-venture members that was also an issuer, asserted that it violated the FCPA's internal controls and books-and-records provisions. The complaint alleged that Technip's internal controls were deficient to detect, deter, and prevent bribery because Technip performed:

- No due diligence on one agent.
- Inadequate due diligence on another agent by only requiring the agent to submit a written questionnaire containing minimal background information.

Although the joint venture, and not Technip, made the payments to the agents involved in the scheme, the SEC's complaint alleged that Technip's books and records contained false information. Senior Technip executives maintained records of the joint venture as a part of Technip's own company records. The SEC alleged those records included contracts used for bribes that were falsely characterized as legitimate consulting and services fees. (Complaint ¶¶ 30-31, *SEC v. Technip*, No. 10-cv-2289 (S.D. Tex. June 28, 2010).)

Ability to Exit Joint Venture

Given the risks associated with foreign joint ventures, the government has urged companies to ensure that they can walk away from ventures or partners that fail to comply with applicable anti-corruption laws. Companies should negotiate for unambiguous language permitting penalty-free departure from a joint venture if a partner violates anti-corruption laws. Without this language, a company could be motivated to remain in a venture and participate in conduct that violates the FCPA. For more information on joint venture exit strategies generally, see Practice Note, Joint Ventures: Exits and Terminations ([8-501-7299](#)).

The DOJ addressed this issue in a May 2001 opinion release regarding a US company's prospective joint venture with a French entity. The DOJ's release procedure enables "issuers and domestic concerns to obtain an opinion of the Attorney General as to whether certain specified, prospective—not hypothetical—conduct conforms with the Department's present enforcement policy regarding the anti-bribery provisions of the [FCPA]" (28 C.F.R. § 80.1). In the May 2001 opinion release, a US company sought guidance on whether the DOJ would pursue an FCPA action regarding a prospective joint venture in which the US company and a French company would each be 50% owners and contribute contracts and transactions. The US company detailed steps it had taken to "avoid a knowing violation of the [FCPA]" and asked whether it would be deemed to have violated the FCPA if one of the contracts the French company contributed was later discovered to have been obtained or maintained through bribery.

The joint venture agreement stated that the US company could terminate or refuse to satisfy its obligations with the prospective French joint venture partner if:

- The French company was convicted of violating France's anti-corruption law.
- The French company entered into a settlement with an admission of liability under French anti-corruption law.
- The US company learned of evidence that the French company violated anti-bribery laws and "that violation, even without a conviction or settlement, [had] a material adverse effect upon the joint venture."

Based on the facts the US company provided detailing its due diligence process for the proposed joint venture and its other precautions to avoid an FCPA violation, the DOJ opined that it did not "intend to take any enforcement action with respect to the [US company's] proposed participation in the joint venture with the French company." The DOJ added a key caveat that it was "concerned that the 'materially adverse effect' standard for terminating the joint venture agreement may be unduly restrictive." According to the DOJ, if the US company's "inability to extricate itself result[s] in [it] taking, in the future, acts in furtherance of the original acts of bribery by the French company, the [US company] may face liability under the FCPA." (DOJ, FCPA Op. Procedure Release No. 2001-01 (May 24, 2001).)

Directors

US directors on a joint venture's board of directors can be liable for offering, making, or authorizing improper payments that violate the FCPA. Foreign directors on the joint venture's board of directors also can be liable for FCPA violations for their conduct in US territory.

When the joint venture involves an SOE, the joint venture is at risk for FCPA liability for the compensation for the directors the SOE appoints if they:

- Have close proximity to government officials.
- Were appointed by government officials.
- Are government officials themselves.
- Have proximity to or influence over:
 - tax regulations;
 - import regulations;

- environmental regulations;
 - public bid processes; or
 - other levers of power that can benefit the joint venture.
- Receive travel reimbursements, board fees, or other funds from the joint venture.

The government may allege that the directors' compensation is an improper payment.

INVESTIGATING ALLEGATIONS OF THIRD-PARTY MISCONDUCT

A company may direct in-house or outside counsel to conduct an internal investigation of allegations of misconduct involving third-party business partners in response to, for example:

- A government industry sweep, which is a wide-ranging government investigation into all companies within a particular industry because the government believes that corruption within the industry is widespread.
- A whistleblower's tip.
- A news report.
- An employee's disclosure.

CHALLENGES INVESTIGATING ALLEGED THIRD-PARTY MISCONDUCT

A company's internal investigation of third-party misconduct can present unique challenges in trying to obtain access to information. Many third parties have no obligation to cooperate with an investigation. Depending on the type of third party, the company may have varying degrees of access to:

- Key individuals.
- Documents.
- Emails.
- Telephone logs.
- Calendar entries.
- Other necessary information.

Counsel should review the company's audit rights relating to the third-party business partner and assess whether other forms of commercial leverage may result in cooperation, for example:

- Refusing to execute future contracts with the third-party supplier.
- Removing the third-party supplier from the company's preferred vendor list.
- Exercising contractual rights, such as, for example, contract termination, indemnification for commercial damages, and claw backs of funds paid.

If the company has limited commercial leverage to persuade the third-party business partner to cooperate with its investigation, the company should:

- Communicate to the third party the steps the company is willing to take if the third party does not assist.
- Document all efforts it took to secure the requested assistance, such as, for example, memorializing telephone calls and meetings and retaining emails.

A record of these communications should be added to the company's due diligence file on the supplier and considered in future contracting decisions. Documenting these efforts also allows the company to describe its internal investigation process to any regulators that later inquire.

The third party's locale also can affect the company's internal investigation. Third parties in distant places can cause logistical difficulties for counsel to visit. Third parties in unsafe locations may be too dangerous for counsel to visit or necessitate that the company provide security for counsel. The local culture, political situation, and local privacy and data protection laws also can prevent access to information.

For more information on investigating FCPA allegations, see Practice Note, Mapping an FCPA Strategy: Internal Investigations and Enforcement Proceedings: Conducting an Internal Investigation ([7-606-5911](#)).

VOLUNTARY SELF-DISCLOSURE

The DOJ and the SEC encourage companies to self-disclose FCPA violations. They also require companies that self-disclose to identify all of the perpetrators both "inside and outside the company." (FCPA Resource Guide, at 54.) A company that is the first to report the conduct to the government and provide information about the third parties involved typically receives the best outcome.

For information about self-reporting FCPA violations to the DOJ, see Legal Update, DOJ Launches FCPA Self-Reporting Pilot Program ([W-001-8495](#)) and Practice Note, Mapping an FCPA Strategy: Internal Investigations and Enforcement Proceedings: Disclosing a Known or Potential Violation ([7-606-5911](#)).

RESOLVING THE INVESTIGATION

In advocating for leniency, a company may leverage information it has regarding third-party business partners to obtain a favorable settlement. For example, the DOJ's DPA with BizJet International Sales and Support Inc. credited BizJet for extraordinary cooperation and agreeing to continue to cooperate in any FCPA investigation of BizJet's conduct or the conduct of its officers, directors, employees, agents, and consultants. (Deferred Prosecution Agreement ¶ 4, *United States v. BizJet Int'l Sales & Support, Inc.*, No. 12-cr-61 (Mar. 14, 2012).)

For more information on resolving FCPA allegations, see Practice Note, Mapping an FCPA Strategy: Internal Investigations and Enforcement Proceedings: Resolving Enforcement Actions ([7-606-5911](#)).

For information on dealing with third parties that have violated the FCPA, see Practice Note, Mapping an FCPA Strategy: Internal Investigations and Enforcement Proceedings: Addressing Third-Party Violations ([7-606-5911](#)).

DOJ GUIDANCE ON COMPLIANCE PROGRAMS AND THIRD-PARTY MANAGEMENT

The US Attorneys' Manual's Principles of Federal Prosecution of Business Organizations lists various factors the government considers when determining whether to bring charges against a corporation. Two of the factors the government considers are:

- The existence and effectiveness of the corporation's pre-existing compliance program.
- The corporation's remedial actions, including any efforts to implement an effective corporate compliance program or to improve an existing one.

(US Attorneys' Manual 9-28.300.)

In 2017, the DOJ's Fraud Section issued guidance regarding key questions the DOJ may ask in evaluating an organization's compliance program. The guidance discusses multiple hallmarks of an effective compliance program, including the company's:

- Tone at the top.
- Compliance policies and procedures.
- Risk assessment processes.
- Program evaluation processes.
- Training.
- Disciplinary procedures.

(DOJ, Evaluation of Corporate Compliance Programs ¶¶ 1-9 (2017).)

The DOJ guidance also includes questions the DOJ may use in assessing a company's management of the third parties it engages, focusing on:

- **Risk-based and integrated processes.** The DOJ evaluates how the company's process to manage third parties has:
 - corresponded to the risks the company identified; and
 - been integrated into the applicable business processes.
- **Appropriate controls.** The DOJ analyzes the actions the company has taken to ensure that:
 - the contract terms describe the services the third party was hired to perform;
 - the payment terms were appropriate;
 - the third party performed the work contracted for; and
 - the third party's compensation was appropriate for the services performed.
- **Management of relationships.** The DOJ assesses how the company has:
 - considered and analyzed the third party's incentive model against compliance risks;
 - monitored the third parties it uses;
 - trained the relationship managers about the compliance risks involved and how to manage them; and
 - incentivized third parties to act ethically and in compliance with all relevant laws.
- **Real actions and consequences.** The DOJ evaluates whether, if the company finds third-party misconduct, the company:
 - identifies red flags from its due diligence of the third party;
 - suspends, terminates, or audits similar third parties due to compliance issues; and
 - monitors future actions to, for example, ensure that the third party is not engaged again after termination.

(DOJ, Evaluation of Corporate Compliance Programs ¶ 10 (2017).)

HOW TO MINIMIZE THIRD-PARTY RISK

To minimize the risks related to working with third parties, companies should:

- Adopt a policy to set clear guidelines when engaging third-party agents and consultants to conduct business outside of the United States on its behalf. This policy should be tailored to the company's specific business and risks (see Standard Document, Policy for the Use of Third-Party Agents Outside of the United States ([2-502-9021](#))).
- Gather information about their third-party business partners through a risk-based due diligence process, focusing on:
 - the reason the third party's services are needed;
 - the third party's qualifications;
 - the third party's associations;
 - the third party's business reputation;
 - the third party's banking and credit status;
 - the third party's relationship, if any, with foreign officials;
 - the payment terms relative to that particular industry and country; and
 - the identification and resolution (if possible) of any corruption red flags.
- (FCPA Resource Guide, at 60.) For more general information, see Practice Note, Risk-Based Due Diligence of Third Parties in Commercial Transactions ([W-004-7864](#)).
- Secure contractual protections, such as audit rights, anti-corruption compliance warranties, and commitments (FCPA Resource Guide, at 60-61). For additional information and sample clauses, see Standard Clauses, General Contract Clauses: Anti-Bribery Representations and Warranties ([W-001-4588](#)) and General Contract Clauses: Anti-Bribery Covenants ([W-001-4742](#)).
- Obtain an annual compliance certificate from third parties to certify compliance with the FCPA and to confirm anti-bribery representations and warranties (see Standard Document, Anti-Bribery Compliance Certificate (Third-Party Intermediaries) ([W-001-5005](#))).
- Negotiate for contractual remedies for potential breach of the contractual provisions, such as:
 - termination;
 - indemnification; and
 - claw back of prior payments made under the contract.
- Educate third parties about the companies' compliance expectations by, for example, providing comprehensive trainings or periodically reviewing the third party's observance of the companies' compliance requirements (FCPA Resource Guide, at 60). For more information and sample training materials, see Standard Documents, Foreign Corrupt Practices Act (FCPA) Training for Employees: Presentation Materials ([2-586-5086](#)) and Foreign Corrupt Practices Act (FCPA) Training Hypotheticals for Employees: Presentation Materials ([0-589-5268](#)).
- Monitor third parties' activities through, for example, regular transaction monitoring or exercising the companies' audit rights. For more information on monitoring third parties, see Practice Note, Developing a Legal Compliance Program: Eight:

Due Diligence and Oversight of Third-Party Relationships
(4-606-5696).

- Document the companies' adherence to compliance controls designed to prevent and, as necessary, detect improper payments by third-party business partners.

Companies that, in the government's view, fail to adhere to their own third-party compliance controls are likely to face more severe penalties if a third party engages in improper conduct. If a company is investigated for third-party misconduct, the company should be prepared to detail the diligent steps it has taken to address and mitigate any risks of third parties making improper payments.

Companies should be prepared to respond to all the applicable questions in the DOJ's 2017 guidance on compliance programs and provide documentary evidence detailing their compliance program, including:

- The structure and staffing of the compliance function.
- Compliance policies, procedures, and related guidance.
- Due diligence files.

- Compliance certifications.
- Compliance communications.
- Training programs.

For comprehensive coverage of compliance programs, see Bribery and Corruption Toolkit (9-502-9452).

Companies also should be prepared to provide quantitative data regarding the compliance program as it applies to third parties, including the number of:

- Third parties on which the companies have performed due diligence.
- Third parties that have participated in anti-corruption compliance training.
- Third-party audits the company conducted.
- Internal investigations or audits relating to third parties.

Without proper documentation and tracking, it is difficult to prove that even the most robust compliance program is operating as it should be.

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call **1-800-733-2889** or e-mail referenceattorneys@tr.com.