FCPA Liability: Minimizing Third-Party Risk

May, 2024 | Contributors: Robert C. Blume and John D. W. Partridge

Companies that transact business internationally with third-party business partners must take steps to minimize potential liability under the Foreign Corrupt Practices Act (FCPA) by identifying high-risk third parties, properly investigating allegations of misconduct, and implementing best practices to address anti-corruption compliance.

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 may provide:

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

However, these same third-party business partners may bring legal and reputational risks 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 US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) are combating this misconduct through enforcement of the FCPA, which prohibits direct corrupt payments made to a foreign official to obtain or retain business, as well as indirect corrupt payments made using third parties. Some of the largest FCPA enforcement actions have involved third-party payments.

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

With few court-imposed bounds and plenty of potentially suspect business arrangements, the DOJ and the SEC have been increasingly attuned to complex schemes involving third parties that act as conduits for improper payments. Given this scrutiny, companies that need to rely on third-party business partners in various parts of the world must understand how the FCPA applies to third-party misconduct when balancing the significant risks and rewards of engaging third-party business partners.

Theories of Liability

The FCPA contains two key components:

- The anti-bribery provisions.
- The accounting provisions.

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

(For the complete version of this resource, which includes more on the FCPA's accounting provisions and on the individuals and entities covered by the FCPA, see FCPA Liability for Third-Party Conduct: Identifying

Pitfalls and Minimizing Risk on Practical Law; for more on the FCPA generally, see The Foreign Corrupt Practices Act: Overview on Practical Law.)

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

- Direct knowledge and participation.
- Authorization.
- Agency.
- Aiding and abetting.
- Conspiracy.

Direct Knowledge of or Participation in Third-Party Misconduct

The government may target a company for the corrupt acts of a third party if the company knew of or participated in the third party's misconduct. Participation can include directing a third-party entity's misconduct. (FCPA Resource Guide, at 28.)

The FCPA defines "knowing" as an awareness or a firm belief of any of the following:

- A person is engaging in the conduct.
- The existence of particular circumstances.
- A particular result is substantially certain to occur. (15 U.S.C. § 78dd-2(h)(3)(A).)

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

The government contends that the FCPA imposes liability on those with actual knowledge of wrongdoing as well as those who purposefully avoid actual knowledge (FCPA Resource Guide, at 23). Courts have agreed and construed knowing to include deliberate ignorance (also called willful blindness or conscious avoidance) (see, for example, *United States v. Kozeny*, 667 F.3d 122, 127-33 (2d Cir. 2011); DOJ Non-Prosecution Agreement, Bio-Rad Laboratories, Inc. (Nov. 3, 2014); DOJ: Press Release, Bio-Rad Laboratories Resolves Foreign Corrupt Practices Act Investigation and Agrees to Pay $14.35 Million Penalty (Nov. 3, 2014)).

Authorization of Third-Party Misconduct

The FCPA's anti-bribery provisions prohibit companies from authorizing a third party to pay any money or give anything of value to a foreign official 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 the company is aware or substantially certain that the third party will offer, give, or promise something of value to a foreign official.

Agency Liability

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 its officers and employees, where the acts are both:

- Undertaken within the scope of the 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.

To determine whether a third party qualifies as a company's agent, the government focuses on the extent of the company's control over the third party. The government considers 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 company 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 28-29.)

The government may establish knowledge by showing that the defendant was aware that there was a high probability of the existence of particular conduct, unless the defendant actually believed the conduct was not occurring.

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

- Subsidiaries (see, for example, Information ¶ 1, United States v. DPC (Tianjin) Co. Ltd., No. 5-cr-482 (C.D. Cal. 2005); In re Alcoa Inc., Admin. Proc. File No. 3-15673 (Jan. 9, 2014)).
- Employees of subsidiaries (see, for example, In re Alcoa Inc., Admin. Proc. File No. 3-15673 (Jan. 9, 2014); *SEC v. Berko,* Compl., No. 20-1789 (E.D.N.Y. June 23, 2021)).
- Attorneys (see, for example, DOJ: Press Release, UK Solicitor Pleads Guilty for Role in Bribing Nigerian Government Officials as Part of KBR Joint Venture Scheme (Mar. 11, 2011)).
- Agents and consultants.

In the *Alcoa* enforcement action, the SEC alleged that Alcoa violated the FCPA because of the conduct of non-issuer subsidiaries, which purportedly acted as Alcoa's agents and, in that capacity, made improper payments to foreign officials (for the complete version of this resource, which discusses the liability of issuers and non-issuers under the FCPA, see FCPA Liability for Third-Party Conduct: Identifying Pitfalls and Minimizing Risk on Practical Law).

To support the agency theory, the SEC asserted that Alcoa exhibited control over the subsidiaries because:

- Alcoa appointed the majority of a subsidiary's strategic council.
- Alcoa set a subsidiary's business and financial goals.
- Alcoa coordinated a subsidiary's legal, audit, and compliance functions.
- The subsidiaries' 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).)

Additionally, in *United States v. Hoskins,* the jury convicted the defendant for, among other things, violating the FCPA by acting as an agent of a US subsidiary when he helped arrange foreign bribes. The district court overturned the defendant's conviction on all of the FCPA charges but upheld the defendant's conviction for money laundering. The court found that while the government showed that the US subsidiary generally controlled the project, the government failed to demonstrate that the US subsidiary had control over the defendant's actions related to procuring consultants sufficient to establish agency under the FCPA. The court reasoned that the government provided no evidence that the US subsidiary had the power to assess the defendant's performance or terminate the defendant's authority to hire consultants. (*United States v. Hoskins,* 2020 WL 914302, at *7-9 (D. Conn. Feb. 26, 2020), aff'd, 44 F.4th 140, 150-52 (2d Cir. 2022) (holding that the evidence was insufficient to show that the US subsidiary exercised control over the scope and duration of its relationship with the defendant).) Although *Hoskins* involved an individual defendant, the court's reasoning also applies to prosecutions of foreign companies.

Aiding and Abetting an FCPA Violation

Under federal law, individuals or companies that aid or abet a crime are considered as culpable as if they had directly committed the crime. Because aiding and abetting is not an independent crime, the government must also prove that a substantive FCPA violation occurred.

To establish aiding and abetting liability, 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, abetted, counseled, commanded, induced, or procured the person who committed the crime.
- The defendant intended to help the commission of the crime. (18 U.S.C. § 2; DOJ: Criminal Resource Manual § 2474 (archived).)

As part of a defendant's association with the criminal conduct, the government must establish that the defendant shared the principal's criminal intent and engaged in some affirmative conduct designed to aid the venture (*United States v. Gallo,* 927 F.2d 815, 822 (5th Cir. 1991)).

Conspiracy to Violate the FCPA

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 that:

- Two or more persons had an agreement to achieve a common objective.
- The objective of the agreement was illegal.
- The defendant knowingly and willfully participated in that agreement.
- Any conspirator committed 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); *United States v. Amiel,* 95 F.3d 135, 144 (2d Cir. 1996)).

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

In certain types of civil conspiracy cases, some courts have applied the intracorporate conspiracy doctrine, which provides that an entity cannot conspire with its employees, officers, agents, or other individuals or entities closely associated with it (see, for example, *Pizza Mgmt., Inc. v. Pizza Hut, Inc.,* 737 F. Supp. 1154, 1165-66 (D. Kan. 1990)). However, some courts have refused to apply the intracorporate conspiracy doctrine to certain types of claims (see *Ashland Oil, Inc. v. Arnett,* 875 F.2d 1271, 1281 (7th Cir. 1989) (refusing to apply the doctrine in an action brought under the Racketeer Influenced and Corrupt Organizations Act); *Stathos v. Bowden,* 728 F.2d 15, 20-21 (1st Cir. 1984) (refusing to apply the doctrine in a civil rights action)).

The overt act does not need to be a criminal act or even a substantial one. Any preparatory step taken that is helpful to the agreement's objective can satisfy the requirement. (See, for example, *Iannelli,* 420 U.S. at 785 n.17 (observing that the overt act can be innocent in nature if it furthers the conspiracy's purpose); *United States v. Khamis,* 674 F.2d 390, 393 (5th Cir. 1982)

(holding that the opening of bank accounts satisfied the overt act requirement).)

In the government's view, a conspiracy charge widens the FCPA's jurisdictional net because the US generally has jurisdiction over all conspirators where at least one conspirator is an issuer or a domestic concern or commits a reasonably foreseeable overt act within the US. The DOJ and the SEC also contend that non-issuer foreign companies may be charged with FCPA violations, including for "reasonably foreseeable [substantive FCPA] crimes committed by a co-conspirator in furtherance of a conspiracy" (FCPA Resource Guide, at 35).

However, the Second Circuit rejected the DOJ's expansive interpretation of the FCPA's jurisdictional sweep and held that the government cannot use theories of conspiracy or complicity to bring FCPA charges against a foreign national unless the foreign national either:

- Was an agent, an employee, an officer, a director, or a shareholder of a US issuer or company.
- Acted illegally while in the US. (*United States v. Hoskins,* 902 F.3d 69, 72, 97 (2d Cir. 2018); but see *United States v. Firtash,* 392 F. Supp. 3d 872, 888-92 (N.D. Ill. 2019) (finding contrary to *Hoskins* that the government does not need to allege that the co-conspirator defendants are part of the class of individuals capable of committing a substantive FCPA violation).)

Penalties for conspiring to violate the FCPA can be as significant as those for a substantive FCPA violation. For example, in December 2016, Rolls-Royce plc entered into a deferred prosecution agreement with the DOJ and agreed to pay a nearly $170 million 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 in exchange for confidential information and contracts. In related proceedings, Rolls-Royce settled with the UK's Serious Fraud Office and Brazil's Ministério Público Federal. In total, Rolls-Royce agreed to pay more than $800 million in criminal penalties. (DOJ: Press Release, Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case (Jan. 17, 2017).)

(For more on conspiracy under 18 U.S.C. § 371, see Conspiracy Charges: Overview and Defending Against a Conspiracy Charge on Practical Law.)

Common Red Flags for Third-Party Business Partners

There are various red flags associated with third-party business partners, such as where:

- Third-party agents or consultants are paid excessive commissions.
- Third-party distributors are given unreasonably large discounts or margins.
- Third-party consulting agreements include only vaguely described services.
- Third-party consultants are in a different line of business than that for which they are engaged.
- The third parties are related to or closely associated with a foreign official.
- The third parties became part of the transaction due to a foreign official's express request.
- The third parties are merely shell companies incorporated in offshore jurisdictions.
- The third parties request payment to offshore bank accounts. (FCPA Resource Guide, at 23.)

(For the complete version of this resource, which provides an in-depth look at common third-party partners and case examples, see FCPA Liability for Third-Party Conduct: Identifying Pitfalls and Minimizing Risk on Practical Law; for an outline of red flags associated with bribery and corruption that can be disseminated through a business as part of a system of anti-bribery or anti-corruption controls, see Bribery and Corruption Red Flags Checklist on Practical Law.)

Minimizing Third-Party Risk

To minimize potential FCPA liability when working with third-party business partners, companies should prioritize the following three compliance objectives:

- Establishing robust and well-documented anti-corruption compliance policies and procedures.
- Researching, conducting due diligence on, auditing, and monitoring third-party business partners.
- Managing contractual risk in agreements with third parties.

Establish Compliance Policies and Programs

To guard against the risks of FCPA liability for third-party misconduct, a company should:

- Collect information from the relevant business unit about the third party and the proposed relationship before engaging the third party (for a model questionnaire, with explanatory notes and drafting tips, see Anti-Bribery Third-Party Risk Assessment: Business Unit Questionnaire on Practical Law).
- Conduct renewal due diligence on third parties periodically, depending on their risk profiles.
- Adopt policies or procedures that set clear guidelines for engaging third-party business partners to conduct business outside the US on the company's behalf. This policy should be tailored to the company's specific business and risks. (For a model policy, with explanatory notes and drafting tips, see Policy for the Use of Third-Party Agents Outside of the United States on Practical Law.)
- Obtain an annual compliance certificate from third-party business partners to certify compliance with the FCPA and confirm anti-bribery representations and warranties (for a model compliance certificate, with explanatory notes and drafting and negotiating tips, see Anti-Bribery Compliance Certificate (Third-Party Intermediaries) on Practical Law).
- Educate third-party business partners about the company's compliance expectations by, for example, providing comprehensive trainings or periodically reviewing the third party's observance of the company's compliance requirements (FCPA Resource Guide, at 60; for model training presentations, with explanatory notes and drafting tips, see Foreign Corrupt Practices Act (FCPA) Training for Employees: Presentation Materials and Foreign Corrupt Practices Act (FCPA) Training Hypotheticals for Employees: Presentation Materials on Practical Law).
- Document the company's adherence to compliance controls that are designed to prevent and, as necessary, detect improper payments by third-party business partners.
- Evaluate the particular risks posed by each third-party business partner so that the company can choose the appropriate outside party to audit and monitor the third-party business partner and provide training to the third-party business partner.
- Periodically monitor and conduct third-party audits of high-risk business partners.

If a company is investigated for third-party misconduct, the company should be prepared to detail the steps it has taken to address and mitigate the risk of improper third-party payments made on the company's behalf. Companies that the government views as having failed to adhere to their own third-party compliance controls are likely to face more severe penalties if a third-party business partner engages in improper conduct.

A company should be prepared to respond to all applicable questions in the DOJ's guidance on compliance programs and provide documentary evidence detailing its own compliance program, including:

- The structure and staffing of the compliance function.
- Compliance policies and procedures, along with related guidance.
- Due diligence files.
- Compliance certifications.
- Compliance communications.
- Training programs.

If a company is investigated for third-party misconduct, the company should be prepared to detail the steps it has taken to address and mitigate the risk of improper third-party payments made on the company's behalf.

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

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

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

(For more on the DOJ's guidance on evaluating the effectiveness of corporate compliance programs, see US Department of Justice Standards for Effective Corporate Compliance Programs on Practical Law; for more on designing anti-bribery and anti-corruption compliance programs, see Bribery Risk in the US: Compliance Roadmap in the November 2023 issue of *Practical Law The Journal*.)

Conduct Risk-Based Due Diligence

Before contracting with any third party, a company should gather information about potential third-party business partners through a risk-based due diligence process. This type of process focuses on:

- The reason the third party's services are needed.
- The third party's actual function (as opposed to their classification or description of the service it would provide).
- The third party's:
  - qualifications;
  - associations (including connections to persons with poor business reputations in the market);
  - business reputation;
  - banking and credit status; and
  - relationships, if any, with foreign officials.
- The proposed payment terms and how they compare to similar arrangements within the particular industry and country.
- The company's identification and resolution (if possible) of any red flags associated with corruption. (FCPA Resource Guide, at 62.)

Before contracting with any third party, a company should gather information about potential third-party business partners through a risk-based due diligence process.

The SEC has brought enforcement actions where companies have allegedly failed to follow their own internal third-party diligence protocols (see, for example, *In the Matter of Amec Foster Wheeler Ltd.*, Release No. 92259, ¶ 1 (June 25, 2021) (finding that a subsidiary used an agent that failed the company's own due diligence process to pay more than $1 million in bribes to obtain a contract with an SOE)).

Companies should therefore monitor and regularly audit their third-party management processes to verify employee compliance and ensure that the protocols effectively identify and resolve any red flags associated with corruption. Companies should not relax the controls and oversight over a third party because that third party has a relationship with the company or with a related entity, such as a third party owned by the company's joint-venture partner. (See, for example, In the Matter of Clear Channel Outdoor Holdings, Inc., SEC Release No. 4466, ¶¶ 1, 19 (Sept. 28, 2023).)

(For more on conducting due diligence of a third party, see Risk-Based Due Diligence of Third Parties in Commercial Transactions on Practical Law.)

Manage Contractual Risk

Companies should negotiate for contractual protections, such as audit rights and anti-corruption compliance warranties and commitments, to facilitate their access to relevant information (FCPA Resource Guide, at 62). After securing these contractual rights, a company should examine each third party's activities through, for example, regular transaction monitoring or exercising the company's audit rights. The company should also perform due diligence before renewing the contract instead of simply automatically renewing the contract.

Additionally, companies should negotiate for contractual remedies for a potential breach of a contractual provision, including:

- Termination.
- Indemnification.
- The clawing back of previous payments made under the contract.

(For model clauses containing anti-bribery and anti-corruption representations and warranties that counsel can use to guard against third-party FCPA liability risk, with explanatory notes and drafting and negotiating tips, see General Contract Clauses: Anti-Bribery Representations and Warranties and General Contract Clauses: Anti-Bribery Covenants on Practical Law; for more on due diligence and the oversight of third-party relationships, see Developing a Legal Compliance Program on Practical Law.)

Reproduced with permission. Published May, 2024. Copyright 2024 by Thomas Reuters http://www.reuters.com