

WHITE COLLAR LITIGATION + INVESTIGATIONS

Combating Bribery and Corruption **Abroad:** What You Need to Know to Protect Your Business

Bribery and Corruption Are Illegal.

What Does That Mean?

Various countries have enacted laws to combat corruption, including the United States, such as the U.S. Foreign Corrupt Practices Act (FCPA), India's Prevention of Corruption Act, the UK Bribery Act of 2010, and the Canadian Corruption of Foreign Public Officials Act.

For U.S. (and many non-U.S.) companies that do business abroad, the FCPA remains a critical and often challenging compliance requirement. The FCPA has two main provisions:

1. **Anti-Bribery:** Prohibits a company, its employees, and its third-party business partners from corruptly offering, paying, promising to pay, or authorizing the payment of money or anything of value to foreign officials to obtain or retain business, influence an official act, or secure an improper advantage.
2. **Financial Record Keeping and Internal Controls:** Requires publicly traded companies to maintain accurate and complete books and records and tailored internal controls to provide a reasonable assurance of the accuracy of financial records and to demonstrate compliance.

A horizontal bar with a gradient from purple to blue.

The FCPA's anti-bribery provision applies to the following:

1. **Issuers**, which is any company, foreign or domestic, with securities registered in the U.S. or required to file reports with the Securities and Exchange Commission (SEC).
2. **Domestic Concerns**, which is any U.S. citizen, national, or resident, and any entity organized under U.S. law or with its principal place of business in the U.S.
3. **Certain persons acting within U.S. territory**, meaning any person or entity who, while in the U.S., uses the mails or an instrumentality of interstate commerce or commits any act in furtherance of a prohibited payment (e.g., calls, emails, faxes, wire transfers through U.S. banks).

COMMON THEORIES OF LIABILITY UNDER THE ANTI-BRIBERY PROVISIONS

The FCPA imposes liability for both direct and indirect violations, meaning companies and individuals can be held liable based on third-party conduct. Below are common theories of liability under which the government pursues FCPA enforcement:

- **Aiding and Abetting:** Whoever aids, abets, counsels, commands, induces, or procures the commission of an FCPA violation is punishable as a principal.
- **Conspiracy:** If two or more persons agree to commit an FCPA offense and any one of them commits an overt act in furtherance of the conspiracy, each conspirator is criminally liable.
- **Agency:** A company may be held liable for bribery committed by its employees, agents, or third-party intermediaries acting within the scope of their authority and for the company's benefit, including where the company acted with willful blindness to the improper conduct.

CURRENT ENFORCEMENT PRIORITIES

The FCPA is enforced by the U.S. Department of Justice (DOJ) and the SEC. Under the current administration, the DOJ has redefined its priorities under the FCPA, focusing on (1) cases in which bribes harm U.S. economic competitiveness abroad; (2) misconduct affecting national security interests; (3) significant corruption, such as systemic bribery, sophisticated concealment, and obstruction of justice; and (4) bribery and corruption linked to cartels and transnational criminal organizations. In June 2025, the SEC expressed that it will follow the DOJ's lead regarding these new priorities.

STATUTE OF LIMITATIONS AND OTHER LAWS: A CONTINUING RISK

While the DOJ's enforcement priorities may evolve, the statute of limitations on FCPA violations means that conduct occurring today can be pursued years from now under a different enforcement climate.

Importantly, conduct that violates the FCPA may also violate the laws of foreign countries or other U.S. local, state or federal laws, such as the U.S. Public Corruption Law (18 U.S.C. § 201), the Travel Act (18 U.S.C. § 1952), the Racketeer Influenced and Corrupt Organizations Act (RICO) (18 U.S.C. §§ 1961 – 1968), campaign finance laws, anti-money laundering laws, and mail and wire fraud laws.

Statute of Limitations:

- **Criminal anti-bribery violations:** Five years.
- **Criminal violations of the books and records/internal controls provision:** Six years.
- **Civil actions:** Five years.

Your Company Does Business Abroad.

What Do You Need to Think About?

Use caution when interacting with foreign government officials or their representatives or other intermediaries: Keep in mind that a “government official” includes employees of state owned/controlled companies, political party officials or candidates, and public international organizations.

“Anything of value” should be interpreted broadly and could include (for example) an internship or job for the government official or his/her family member. It can also include small payments or non-cash benefits, and even small value items or dollar amounts can create liability if part of a pattern of conduct.

Conduct a risk assessment: Conduct a tailored, enterprise-wide risk assessment to identify key compliance threats to your business, such as (1) operations in high-risk jurisdictions or with high-risk business partners; (2) procurement, management, and execution of government contracts and third-party relationships; and (3) financial and accounting controls.

Design and enforce anti-bribery and anti-corruption policies: Put in place and enforce policies that are tailored to the risk assessment and the specific needs of the business, covering areas like conflicts of interest, facilitating payments, compliance with local laws, gifts and entertainment, sponsorships, donations, intermediaries, and goods and services not priced to reflect fair value where there may be corruption risk.

Prohibit cash payments or set cash payment limits: Cash is hard to trace and widely accepted, making it the primary transaction mechanism for financial crimes. Implementing cash limits or prohibiting cash payments altogether can deter bad actors from making improper payments.

Train employees and provide continuing, accessible education: Periodically deliver tailored, role-specific training to key employees using diverse formats suited to the audience’s characteristics.

Maintain accurate and complete books and records:

To ensure financial integrity, accurately record transactions to reflect true business activities, maintain internal accounting controls to safeguard assets and ensure reliable financial statements, and prevent falsification of records, including off-the-books accounts or disguised payments.

Vet third-party business partners: Conduct risk-based due diligence before engaging third parties by vetting their qualifications and reputation, and the structure of the relationship itself (e.g., compensation), and refresh due diligence as risks evolve.

Require business partners to abide by your company’s values and comply with the law: Your company can be held responsible for violations by business partners if you do not take reasonable steps to align on compliance. Requiring fair, transparent payment terms, full compliance, audit rights, and clear consequences for misconduct are examples of how agreement terms can promote compliance.

Establish a confidential reporting structure: Maintain secure, well-publicized hotlines or similar reporting channels that allow anonymous, confidential submissions, and enforce clear whistleblower and anti-retaliation policies.

Conduct periodic reviews of your compliance program: Conduct periodic program reviews and control testing to identify weaknesses in your compliance program and implement timely improvements to policies, controls, and training based on risk assessment results, employee feedback, reporting trends, or changes in the business or the law.

Encourage and foster a culture of compliance: Ensure that senior leadership communicates a zero-tolerance stance on misconduct; assign clear responsibility for policy oversight, training, and enforcement; and allocate sufficient resources to continuously enhance compliance efforts.

You Have Concerns That There Might Be a Violation.

What Do You Do?

CONDUCT AN INTERNAL INVESTIGATION

If you believe that a violation of the FCPA or related law may have occurred, conducting an internal investigation is imperative. A thorough and objective investigation may mitigate the risk of liability or minimize damages; whereas a failure to investigate or an incomplete investigation may result in stiffer penalties. Preserve any documents related to the potential violation, including hard-copy documents, emails, text messages, files, etc. Additionally, consider engaging outside counsel to maintain attorney-client privilege.

For publicly traded companies, audit committee charters often give the audit committee oversight over internal investigations and require that they be conducted by independent outside counsel. The primary audience for those investigations are outside auditors, who should be consulted to ensure transparency and avoid duplicating efforts.

Ensure that investigations of complaints:

- Are routed to **qualified, independent personnel**;
- Are properly scoped, objective, and **timely documented**; and
- Include **appropriate follow-up, discipline, or remediation when needed**.

CONSIDER YOUR DISCLOSURE OBLIGATIONS

A potential FCPA violation may trigger a reporting requirement to a company's Directors & Officers (D&O) Liability Insurance or similar carriers. If you have credible evidence of a potential FCPA violation or other related law, consider discussing it with your D&O insurance consultant or broker.

For publicly traded companies, the Sarbanes-Oxley Act and related securities laws impose certification and reporting requirements that may require consideration of disclosure of potential FCPA issues to external auditors, the company's audit committee, or, in some circumstances, regulators. See 15 U.S.C. § 7241; see *also* Securities Exchange Act Rule 10A-3; 15 U.S.C. § 7245.

When to consider notifying external auditors and/or audit committees:

1. When credible evidence suggests a potential violation of the FCPA, particularly where financial records or reporting may be inaccurate or misleading.
2. When the matter involves senior management or significant financial exposure.
3. If internal investigations reveal systemic control weaknesses or recurring compliance lapses that may impact financial reporting or audit integrity.

Depending on the facts and materiality, public companies may also need to consider whether public disclosure is required under applicable SEC reporting requirements.

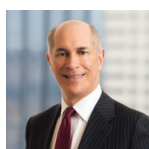
CONSIDER WHETHER YOU SHOULD SELF-DISCLOSE THE VIOLATION TO THE SEC OR THE DOJ

Both the DOJ and the SEC provide incentives for companies that self-disclose potential FCPA violations or cooperate with a government investigation. Companies that promptly self-disclose, fully cooperate, remediate, and present no aggravating circumstances can receive declinations of prosecution, which can result in a significant reduction of financial penalties.

Key actions that help secure credibility and cooperation with government agencies include:

1. **Self-Policing:** Maintain strong compliance measures before any misconduct is discovered.
2. **Self-Reporting:** Report any known misconduct fully, promptly, and transparently.
3. **Remediation:** Implement corrective actions, such as disciplining involved parties and enhancing controls.
4. **Cooperation:** Provide authorities with relevant information, documents, and reasonable access to facilitate their investigations.

Key Contacts



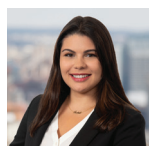
Jay Dubow
Partner
Philadelphia
jay.dubow@troutman.com
215.981.4713



Abigail Hazlett
Partner
Philadelphia
abigail.hazlett@troutman.com
215.981.4578



Peter Jeydel
Partner
Washington, D.C.
peter.jeydel@troutman.com
202.274.2962



Isabela P. Herlihy
Associate
Philadelphia
isabela.herlihy@troutman.com
215.981.4680



Anthony Osticco
Associate
Philadelphia
anthony.osticco@troutman.com
215.981.4770