

# Third-Party Intermediary FCPA Exposures

## *Mitigating the Risks*

### *Part Two of a Two-Part Article*

By Mehreen Zaman

*Editor's Note: In last month's newsletter, the author shone a light on an issue that might be overlooked by some companies doing business overseas: the risk that a third party a business works with — like a consultant, agent, broker or distributor — will involve the company, perhaps unknowingly, in activities that could expose it to liability for violations of the the Foreign Corrupt Practices Act (FCPA), the government's primary weapon against bribery of foreign officials. That discussion concludes herein.*

#### THE DOJ'S NEW PILOT FCPA ENFORCEMENT PLAN

The Department of Justice's (DOJ's) April 5, 2016, memorandum titled The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance ("Enforcement Plan"), sets out several major FCPA enforcement initiatives. See <http://1.usa.gov/1TuEjkh>.

**Mehreen Zaman** (mzaman@postschell.com) works out of Philadelphia as a senior associate in the Internal Investigations and White Collar Defense Group of Post & Schell, P.C., with a focus on FCPA and export matters.

First, the DOJ is "intensifying" its efforts by adding 10 prosecutors to its FCPA Unit, supported by three new dedicated squads of FBI special agents and increased information-sharing with foreign counterparts.

Second, it establishes a one-year FCPA enforcement "pilot program," effective April 5, 2016, to "promote greater accountability for individuals and companies that engage in corporate crime by motivating companies to voluntarily self-disclose FCPA-related misconduct, fully cooperate with the Fraud Section, and where appropriate, remediate flaws in their controls and compliance programs."

Under the pilot program, companies can receive defined cooperation credit in FCPA cases if they: 1) voluntarily self-disclose FCPA violations; 2) cooperate fully with the DOJ's investigation, including, unless legally prohibited, by facilitating the third-party production of documents and witnesses; and 3) remediate any compliance issues that led to the FCPA violation. The Enforcement Plan acknowledges that what qualifies as appropriate cooperation and remediation is case-specific. It does list some familiar general criteria for an "effective compliance and ethics program,"

such as dedicating sufficient resources to the compliance function, ensuring the independence of the compliance function and auditing the compliance program to assure its effectiveness.

If a company voluntarily self-discloses its misconduct and meets the requirements of the pilot program, the DOJ may accord up to a 50% reduction off the bottom end of the Sentencing Guidelines fine range, generally will not require the appointment of a monitor if an effective compliance program is in place, and will consider declining prosecution. If a company does not voluntarily self-disclose its misconduct, but later fully cooperates and remediates, the DOJ will accord, at most, a 25% reduction off the bottom end of the Sentencing Guidelines fine range. Note that, to qualify for any mitigation credit under this pilot program, the company "should be required" to disgorge all profits from the FCPA misconduct.

#### MITIGATING RISK: COMMON RED FLAGS

In its FCPA Resource Guide, the government cites eight red flags associated with the use of third parties:

1. Excessive commission payments to third-party agents or consultants;

2. Unreasonably large discounts to third-party distributors;
3. Third-party "consulting agreements" that include only vaguely described services;
4. The third-party consultant is in a different line of business than that for which it has been engaged;
5. The third party is related to or closely associated with the foreign official;
6. The third party became part of the transaction at the express request or insistence of the foreign official;
7. The third party is merely a shell company incorporated in an offshore jurisdiction; and
8. The third party requests payment to offshore bank accounts.

Upfront due diligence to unearth these or other similar issues is necessary and expected by the government. While the extent of due diligence will vary by the size and resources of the particular business, industry sector, market and transaction type, there are some basic steps to consider in mitigating FCPA exposures.

#### **DUE DILIGENCE**

Recommended elements of a due diligence system, include:

- 1. Conducting a risk assessment.** Companies should conduct a risk assessment for hiring, retaining and overseeing a third party. This includes validating the business rationale for hiring the third party, learning about its reputation and government affiliations, assessing the types of interactions it may have with government officials, and determining who will be interacting with government officials and in what capacity.
- 2. Having clearly written, policies and procedures that are reviewed and updated regularly.** A company should establish clear,

written due diligence policies, and these policies should be updated periodically. Companies must ensure that due diligence is conducted for every third-party intermediary.

**3. Having written contracts with FCPA terms.** Contract terms should identify exactly what services are being performed by the third party and what (fair market value) compensation will be paid. The contract should include audit and cooperation provisions (discussed below) as well certifications that the third party is aware of the FCPA and local prohibitions in this area and will not violate them.

**4. Monitoring and auditing third parties.** Third parties should be monitored to ensure that they are performing the services agreed to under the contract and that they are doing so legally. Companies should require regular invoices from third parties that detail the work they are doing, and should consider periodic audits of third parties' books to vet expenditures.

**5. Addressing issues immediately.** Ignorance and avoidance are not defenses under the FCPA. If a company suspects a third-party corruption issue, it must investigate promptly. The investigation should be documented. Failure to cooperate in such an investigation, should result in termination of the third party contract. Any company employee determined to be in violation of the company's FCPA policy should be subject to prompt and appropriate training and discipline.

**6. Assigning senior corporate executives of the company to oversee the anti-corruption and due diligence programs.** Assigning a dedicated executive to coordinate anti-corruption matters, with the authority to report directly to the CEO and Board, can

minimize the risk of having FCPA issues fall through the cracks due to a lack of a clear decision-making structure. Alstom, Avon and ADM agreed to create such a position as part of their resolutions with the government. Additionally, the DOJ's new FCPA Enforcement Plan, discussed below, makes it clear that the government expects companies to have qualified and experienced compliance personnel who are afforded the necessary independence to perform their duties.

**7. Training third-party intermediaries.** In addition to training employees on due diligence and anti-corruption policies, businesses should consider training third-party intermediaries in order to help ensure understanding of the law, reduce the risk of FCPA violations and signal to the government that the company is doing everything it can to avoid improper third-party payments to foreign officials.

#### **CONCLUSION**

The FCPA Enforcement Plan reinforces the government's resolve to prosecute individuals and companies for FCPA violations committed through third party intermediaries. While there is no ironclad way to prevent third-party intermediaries from violating the FCPA, risks can be mitigated. A robust due diligence system to vet potential third-party intermediaries, and timely investigations of potential issues if they arise, provide the best chance of avoiding, or at least minimizing, FCPA exposure.

